

(19)日本国特許庁 (J P)

(12) 公表特許公報(A)

(11)特許出願公表番号
特表2001-519562
(P2001-519562A)

(43) 公表日 平成13年10月23日(2001.10.23)

(51) Int.Cl. ⁷	識別記号	F I	テ-マコト ⁸ (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 F 5 B 0 1 7
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B 5 D 0 4 4
G 1 1 B 20/10		G 1 1 B 20/10	D 5 J 1 0 4
	3 2 1		3 2 1 Z

審查請求 未請求 予備審查請求 有 (全 71 頁)

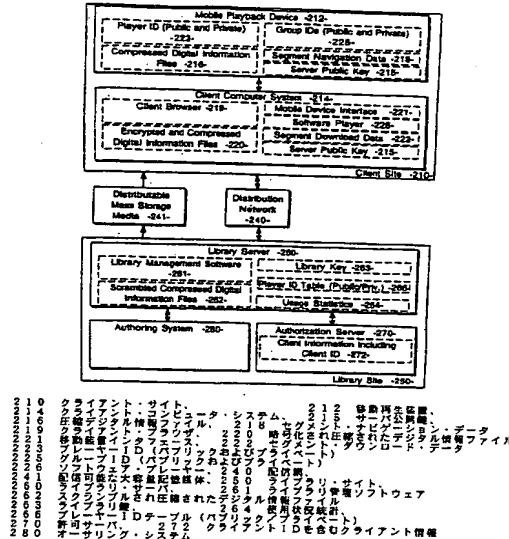
(21)出願番号	特願2000-515227(P2000-515227)	(71)出願人	オーディブル・インコーポレーテッド アメリカ合衆国・07470・ニュージャージ イ洲・ウェイン・ウイロウブルック ブル ーバード・65
(86) (22)出願日	平成10年10月2日(1998.10.2)	(72)発明者	モット、ティモシイ アメリカ合衆国・83340・アイダホ州・ケ ッチャム・ピーオーボックス 6289・オー ルド ミル ロード・110
(85)翻訳文提出日	平成12年4月3日(2000.4.3)	(72)発明者	ストーリイ、ガイ アメリカ合衆国・10012・ニューヨーク 州・ニューヨーク・スプリング ストリー ト・151
(86)国際出願番号	PCT/US98/20659	(74)代理人	弁理士 山川 政樹
(87)国際公開番号	WO99/18506		
(87)国際公開日	平成11年4月15日(1999.4.15)		
(31)優先権主張番号	08/943,582		
(32)優先日	平成9年10月3日(1997.10.3)		
(33)優先権主張国	米国(US)		

最終頁に統く

(54) 【発明の名称】 デジタル情報再生装置をターゲティングする方法と装置

(57) 【要約】

デジタル情報再生装置（212）をターゲティングする方法、装置、および製品。再生装置に装置ID（223）および／またはグループID（225）が埋め込まれる。デジタル情報ファイル（216）にも装置IDまたはグループIDが埋め込まれる。デジタル情報ファイルが受信されると、再生装置の装置IDまたはグループIDが、デジタル情報ファイルに含まれる装置IDまたはグループIDと比較される。次いで、デジタル情報ファイルの装置IDまたはグループIDが再生装置の装置IDまたはグループIDと一致する場合、デジタル情報ファイルが再生される。



【特許請求の範囲】

【請求項1】 デジタル情報再生装置をターゲティングする方法であって、
再生装置に第1の装置識別子を埋め込むステップと、
デジタル情報ファイルに第2の装置識別子を埋め込むステップと、
再生装置にデジタル情報ファイルを与えるステップと、
第1の装置識別子と第2の装置識別子を比較するステップと、
第1の装置識別子が第2の装置識別子と一致する場合にデジタル情報ファイル
を再生するステップと
を含むことを特徴とする方法。

【請求項2】 第1の装置識別子を埋め込むステップが、再生装置に固有の
識別子を埋め込むステップを含むことを特徴とする請求項1に記載の方法。

【請求項3】 第2の装置識別子を埋め込むステップが、デジタル情報ファ
イルのヘッダ・ブロックに第2の装置識別子を埋め込むステップを含むことを特
徴とする請求項1に記載の方法。

【請求項4】 さらに、デジタル署名アルゴリズムを実行してヘッダ・ブロ
ックを認証するステップを含むことを特徴とする請求項3に記載の方法。

【請求項5】 さらに、
デジタル情報ファイルのあるセクションの第1のコード化値を算出するステッ
プと、
デジタル情報ファイルに第1のコード化値を埋め込むステップと、
再生装置にデジタル情報ファイルが与えられるときに第2のコード化値を算出
するステップと、
第1のコード化値が第2のコード化値と一致する場合にデジタル情報ファイル
を再生するステップとを含むことを特徴とする請求項1に記載の方法。

【請求項6】 第1のコード化値を埋め込むステップが前記セクションに安
全ハッシュ値を埋め込むステップを含むことを特徴とする請求項5に記載の方法
。

【請求項7】 さらに、
再生装置に第1のグループ識別子を記録するステップと、

デジタル情報ファイルに第2のグループ識別子を埋め込むステップと、
第1のグループ識別子と第2のグループ識別子を比較するステップと、
第1のグループ識別子が第2のグループ識別子と一致する場合に、デジタル情
報ファイルを再生するステップとを含むことを特徴とする請求項1に記載の方法

【請求項8】 第1のグループ識別子を記録するステップが、グループ識別
子をリモート電子供給源から電子的に受信するステップを含むことを特徴とする
請求項7に記載の方法。

【請求項9】 第2のグループ識別子を埋め込むステップが、デジタル情報
ファイルのヘッダ・ブロックに第2のグループ識別子を埋め込むステップを含む
ことを特徴とする請求項7に記載の方法。

【請求項10】 さらに、デジタル署名アルゴリズムを実行してヘッダ・ブ
ロックを認証することを特徴とする請求項9に記載の方法。

【請求項11】 さらに、デジタル署名アルゴリズムを実行してデジタル情
報ファイルを認証することを特徴とする請求項1に記載の方法。

【請求項12】 さらに、デジタル署名アルゴリズムを実行してデジタル情
報ファイルのあるセクションを認証することを特徴とする請求項1に記載の方法

【請求項13】 キーボード、ポインティング・デバイス、ビジュアル・デ
ィスプレイ、およびデータ記憶装置を有し、デジタル情報再生装置をターゲティ
ングするコンピュータ・システムで使用される、コンピュータ使用可能媒体を備
えた製品であって、その媒体にはコンピュータ可読プログラム・コードが記録さ
れており、そのプログラム・コードが、

コンピュータに、再生装置に第1の装置識別子を埋め込ませるように、コン
ピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードと、
コンピュータに、デジタル情報ファイルに第2の装置識別子を埋め込ませるよ
うに、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コ
ードと、

コンピュータによって、再生装置にデジタル情報ファイルを与えるように、コ

ンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードと、コンピュータに第1の装置識別子と第2の装置識別子を比較させるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードと、第1の装置識別子が第2の装置識別子と一致する場合に、コンピュータにデジタル情報ファイルを再生させるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードとを含むことを特徴とする製品。

【請求項14】 コンピュータに第1の装置識別子を埋め込ませるコンピュータ可読プログラム・コードが、コンピュータに再生装置に固有の識別子を埋め込ませるためにコンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードを含むことを特徴とする請求項13に記載の製品。

【請求項15】 コンピュータに第2の装置識別子を埋め込ませるコンピュータ可読プログラム・コードが、コンピュータに、デジタル情報ファイルのヘッダ・ブロックに第2の装置識別子を埋め込ませるようにコンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードを含むことを特徴とする請求項13に記載の製品。

【請求項16】 さらに、コンピュータに、デジタル署名アルゴリズムを実行してヘッダ・ブロックを認証するように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードを含むことを特徴とする請求項15に記載の製品。

【請求項17】 さらに、コンピュータに、デジタル情報ファイルのあるセクションの第1のコード化値を算出せしように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードと、

コンピュータに、デジタル情報ファイルに第1のコード化値を埋め込ませるよう、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードと、

再生装置にデジタル情報ファイルが与えられるときに、コンピュータに第2のコード化値を算出せしように、コンピュータ使用可能媒体に記録されたコンピ

ュータ可読プログラム・コードと、

第1のコード化値が第2のコード化値と一致する場合に、コンピュータにデジタル情報ファイルを再生させるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードとを含むことを特徴とする請求項13に記載の製品。

【請求項18】 コンピュータに第1のコード化値を埋め込ませるコンピュータ可読プログラム・コードが、コンピュータに、前記セクションに安全ハッシュ値を埋め込ませるようにコンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードを含むことを特徴とする請求項17に記載の製品。

【請求項19】 さらに、

コンピュータに、再生装置に第1のグループ識別子を埋め込ませるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードと、コンピュータに、デジタル情報ファイルに第2のグループ識別子を埋め込ませるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードと、

コンピュータに、第1のグループ識別子と第2のグループ識別子を比較させるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードと、

第1のグループ識別子が第2のグループ識別子と一致する場合に、コンピュータにデジタル情報ファイルを再生させるようにコンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードとを含むことを特徴とする請求項13に記載の製品。

【請求項20】 コンピュータに第1のグループ識別子を埋め込ませるコンピュータ可読プログラム・コードが、コンピュータに、グループ識別子をリモート電子供給源から電子的に受信させるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードを含むことを特徴とする請求項19に記載の製品。

【請求項21】 コンピュータに第2のグループ識別子を埋め込ませるコンピュータ可読プログラム・コードが、コンピュータに、デジタル情報ファイルの

ヘッダ・ブロックに第2のグループ識別子を埋め込ませるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードを含むことを特徴とする請求項19に記載の製品。

【請求項22】 さらに、コンピュータに、デジタル署名アルゴリズムを実行してヘッダ・ブロックを認証させるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードを含むことを特徴とする請求項21に記載の製品。

【請求項23】 さらに、コンピュータに、デジタル署名アルゴリズムを実行してデジタル情報ファイルを認証させるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードを含むことを特徴とする請求項13に記載の製品。

【請求項24】 さらに、コンピュータに、デジタル署名アルゴリズムを実行してデジタル情報ファイルのあるセクションを認証させるように、コンピュータ使用可能媒体に記録されたコンピュータ可読プログラム・コードを含むことを特徴とする請求項13に記載の製品。

【請求項25】 デジタル情報再生装置をターゲティングするシステムであつて、

再生装置に第1の装置識別子を埋め込む第1の再生手段を有するデジタル・コンピュータと、

デジタル情報ファイルに第2の装置識別子を埋め込むようにデジタル・コンピュータによって操作される第2の埋込み手段と、

再生装置にデジタル情報ファイルを与えるためにデジタル・コンピュータに論理的に結合された手段と、

第1の装置識別子と第2の装置識別子を比較するようにデジタル・コンピュータによって操作される比較手段と、

第1の装置識別子が第2の装置識別子と一致する場合にデジタル情報ファイルを再生するためにデジタル・コンピュータに論理的に結合された再生手段とを備えることを特徴とするシステム。

【請求項26】 第1の埋込み手段がさらに、再生装置に固有の識別子を埋

め込む手段を備えることを特徴とする請求項25に記載のシステム。

【請求項27】 第2の埋込み手段がさらに、デジタル情報ファイルのヘッダ・ブロックに第2の装置識別子を埋め込む手段を備えることを特徴とする請求項25に記載のシステム。

【請求項28】 さらに、デジタル署名アルゴリズムを実行してヘッダ・ブロックを認証するようにデジタル・コンピュータによって操作される認証手段を備えることを特徴とする請求項27に記載のシステム。

【請求項29】 さらに、
デジタル情報ファイルのあるセクションの第1のコード化値を算出するように
デジタル・コンピュータによって操作される手段と、
デジタル情報ファイルに第1のコード化値を埋め込むようにデジタル・コンピュータによって操作される手段と、
再生装置にデジタル情報ファイルが与えられるときに第2のコード化値を算出
するようにデジタル・コンピュータによって操作される手段と、
第1のコード化値が第2のコード化値と一致する場合にデジタル情報ファイル
を再生するようにデジタル・コンピュータによって操作される手段とを備えるこ
とを特徴とする請求項25に記載のシステム。

【請求項30】 第1の埋込み手段がさらに、前記セクションに安全ハッシュ
値を埋め込む手段を備えることを特徴とする請求項29に記載のシステム。

【請求項31】 さらに、
再生装置に第1のグループ識別子を記録するようにデジタル・コンピュータに
よって操作される手段と、
デジタル情報ファイルに第2のグループ識別子を埋め込むようにデジタル・コンピュータによって操作される手段と、
第1のグループ識別子と第2のグループ識別子を比較するようにデジタル・コンピュータによって操作される手段と、
第1のグループ識別子が第2のグループ識別子と一致する場合にデジタル情報
ファイルを再生するようにデジタル・コンピュータによって操作される手段とを
備えることを特徴とする請求項25に記載のシステム。

【請求項 3 2】 第 1 のグループ識別子を記録する手段がさらに、グループ識別子をリモート電子供給源から電子的に受信する手段を備えることを特徴とする請求項 3 1 に記載のシステム。

【請求項 3 3】 第 2 のグループ識別子を埋め込む手段がさらに、デジタル情報ファイルのヘッダ・ブロックに第 2 のグループ識別子を埋め込む手段を備えることを特徴とする請求項 3 1 に記載のシステム。

【請求項 3 4】 さらに、デジタル署名アルゴリズムを実行してヘッダ・ブロックを認証するようにデジタル・コンピュータによって操作される手段を備えることを特徴とする請求項 3 3 に記載のシステム。

【請求項 3 5】 さらに、デジタル署名アルゴリズムを実行してデジタル情報ファイルを認証するようにデジタル・コンピュータによって操作される手段を備えることを特徴とする請求項 2 5 に記載のシステム。

【請求項 3 6】 さらに、デジタル署名アルゴリズムを実行してデジタル情報ファイルのあるセクションを認証するようにデジタル・コンピュータによって操作される手段を備えることを特徴とする請求項 2 5 に記載のシステム。

【請求項 3 7】 オーディオ再生装置をターゲティングするシステムであつて、

オーディオ・ファイルに装置識別子を埋め込む第 1 の埋込み手段を有するデジタル・コンピュータと、

オーディオ・ファイルにグループ識別子を埋め込むようにデジタル・コンピュータによって操作される第 2 の埋込み手段と、

再生装置にオーディオ・ファイルを与えるためにデジタル・コンピュータに論理的に結合された手段と

を備えることを特徴とするシステム。

【発明の詳細な説明】**【0001】****(発明の分野)**

本発明は、全般的にはデジタル情報送信、受信、再生システムに関し、詳細には、デジタル情報再生装置をターゲティングする方法および装置に関する。

【0002】**(発明の背景)**

デジタル・データの圧縮およびコンピュータ・システムの記憶機能の拡張における最近の技術的発展と、コンピュータ・ネットワーク・インフラストラクチャの帯域幅の増大によって、大量のデジタル情報への個人的なアクセスおよびそのような情報の使用についての新たな可能性が生まれている。この種のデジタル情報の一形態は、コンピュータ・ネットワークを介してデジタル化情報として供給されるオーディオ情報である。

【0003】

対話型デジタル情報送信、受信、再生システムの分野で、本出願人にはいくつかの特許が知られている。1992年7月21日にYurt等に発行された米国特許第5,132,992号(Yurt)は、デジタル信号処理を使用して高データ圧縮率を実現することによってビデオおよび／またはオーディオ情報を配信するシステムについて説明している。Yurt特許は、ソース・マテリアル・ライブラリから得たアイテムをフォーマット済みデータとして所定のフォーマットにする変換手段を含む送信システムについて説明している。オーディオ・データは適応差分パルス符号変調(ADPCM)プロセスをオーディオ・データに適用することによってオーディオ・コンプレッサによって圧縮される。記憶されたアイテムは、記憶コード化中に各アイテムに割り当てられる固有のアドレス・コードを使用することによって圧縮データ・ライブラリにおいてアクセスされる。この固有のアドレス・コードは、Yurt送受信プロセス全体にわたって情報およびアイテムを要求しそれらにアクセスするために使用される。Yurt送信システムは、システムがユーザ・アカウントにアクセスするための顧客識別子(ID)コードをユーザが入力するための手段を含み、ユーザがシステムの加入者であ

ることをシステムに示す。加入者に問題がない場合、Yurt システムは、前述の技法を使用して、選択されたタイトルを供給する。

【0004】

Yurt に記載されたオーディオ送受信システムの 1 つの重要な問題は、デジタル情報ライブラリのセキュリティと、デジタル情報ライブラリからユーザにダウンロードされるアイテムのセキュリティとを確保する有効な手段がないことである。Yurt は、ライブラリ内のアイテムに割り当てられる固有の ID コードと、特定のユーザに割り当てられる顧客 ID コードとの使用法について説明しているが、クローン・ライブラリを許可なしで作成するか、あるいはライブラリ・アイテムを許可なしでダウンロードまたはコピーするのを防止する認証プロトコルや暗号化技法については説明していない。第 2 に、Yurt および関連する従来技術は、移動再生装置のインターフェースを有するクライアント・コンピュータ・システムをサポートするサーバ・ベースのデジタル情報ライブラリとの間で安全なトランザクションを行う認証手段や暗号化手段については説明していない。第 3 に、従来技術は、確認すべきデジタル情報パッセージを選択する機構について説明していない。従来技術のシステムは、移動再生装置でどのくらいの記憶空間が使用できるかに応じてプログラムの一部のみをクライアント・コンピュータ・システムから移動再生装置にダウンロードするためのシステムについても説明していない。従来技術のシステムは、デジタル情報ライブラリから移動再生装置にダウンロードすべき複数のプログラムを指定する機能についても説明していない。従来技術のシステムは、デジタル情報ライブラリのコンテンツを生成するためにオーサリング・システムで必要とされるプロセスについて詳しく説明していない。最後に、従来技術のシステムは、ライブラリ・コンテンツ・プロバイダが、ライブラリ・アイテムのアクセスに関する使用情報に対する問合せをリアルタイムに実行するためのアカウント・システムについても説明していない。

【0005】

(発明の概要)

本発明は、デジタル情報再生装置をターゲティングする方法、装置、および製品を提供する。装置 ID またはグループ ID が再生装置に組み込まれる。デジタル

ル情報ファイルにも装置IDまたはグループIDが組み込まれる。デジタル情報ファイルが受信された後、再生装置の装置IDまたはグループIDが、デジタル情報ファイルに含まれる装置IDまたはグループIDと比較される。次いで、デジタル情報ファイルの装置IDまたはグループIDが再生装置の装置IDまたはグループIDと一致する場合、このデジタル情報ファイルが再生される。

【0006】

本発明は、添付の図面を参照して例として示され、限定的なものではない。同じ参考番号は同様の要素を示す。

【0007】

(本発明の好ましい実施形態の詳細な説明)

本発明の好ましい実施形態は、クライアント・コンピュータ・システムおよびクライアント・コンピュータ・システムに着脱可能に接続することのできる移動デジタル情報再生システムにデジタル情報ライブラリ・プログラムを安全に転送するために認証プロトコル、ターゲティング・プロトコル、および暗号化プロトコルを使用するコンピュータ・ネットワーク・ベースのデジタル情報ライブラリ・システムである。以下の詳細な説明では、本発明を完全に理解していただくために多数の特定の詳細について述べる。しかし、当業者には、これらの特定の詳細を使用しなくとも本発明を実施できることが明らかになろう。他の例では、本発明を必要に曖昧にしないように、周知の構造、インターフェース、およびプロセスは詳しく示していない。

【0008】

図1は、本発明の一実施形態が実現される典型的なデータ処理システムを示す。しかし、当業者には、様々なシステム・アーキテクチャの他の代替システムも使用できることが明らかになろう。図1に示すデータ処理システムは、情報を伝達するバスまたはその他の内部通信手段101と、情報を処理するためにバス101に結合されたプロセッサ102とを含む。システムはさらに、情報およびプロセッサ102によって実行される命令を記憶するためにバス101に結合されたランダム・アクセス・メモリ(RAM)またはその他の揮発性記憶装置104(メイン・メモリと呼ばれる)を備える。メイン・メモリ104は、プロセッサ

102によって命令が実行される間に一時変数または他の中間情報を記憶するために使用することもできる。システムは、プロセッサ102用の静的情報および命令を記憶するためにバス101に結合された読み取り専用メモリ（ROM）および／または静的記憶装置106と、磁気ディスク・ドライブや光ディスク・ドライブなどの大容量記憶装置107も備える。大容量記憶装置107は、バス101に結合され、通常は、情報および命令を記憶するために磁気ディスクや光ディスクなどのコンピュータ可読大容量記憶媒体108と共に使用される。システムはさらに、コンピュータ・ユーザに情報を表示するためにバス103を介してバス101に結合された陰極線管（CRT）や液晶ディスプレイ（LCD）などの表示装置121に結合することができる。情報およびコマンド選択肢をプロセッサ102に伝達するために、英数字キーおよびその他のキーを含む英数字入力装置122をバス103を介してバス101に結合することもできる。追加のユーザ入力装置としては、バス103を介してバス101に結合されたマウスや、トラックボールや、スタイルスや、カーソル方向キーなどのカーソル制御装置123がある。これらで方向情報およびコマンド選択肢をプロセッサ102に伝達し表示装置121上のカーソル移動を制御する。任意選択でバス103を介してバス101に結合できる他の装置は、紙、フィルム、または同様な種類の媒体などの媒体上に命令、データ、またはその他の情報を印刷するために使用できるハード・コピー装置124である。好ましい実施形態では、通信装置125は、ネットワーク・コンピュータ・システムの他のノードまたは他のコンピュータ周辺装置にアクセスする際に使用できるようにバス103を介してバス101に結合される。この通信装置125は、イーサネット、トーカン・リング、インターネット、またはワイド・エリア・ネットワークに結合するために使用されるようないくつかの市販のネットワーク化周辺装置のうちの任意の周辺装置を含むことができる。通信装置125は、スキャナや、端末や、専用プリンタや、オーディオ入出力装置などのリモート・コンピュータ周辺装置と通信するように設計された任意の数の市販の周辺装置を含むこともできる。通信装置125は、RS232またはその他の従来型のシリアル・ポート、従来型のパラレル・ポート、SCSIポート、またはその他のデータ通信手段を含むこともできる。通信装置125は

、赤外線IRDAプロトコルや、スペクトラム拡散や、無線LANなどの無線データ転送装置手段を使用することができる。また、通信装置125は好ましい実施形態では、以下で詳しく説明するように移動再生装置212をクライアント・コンピュータ・システム214に結合するために使用される。好ましい実施形態で使用される他の1つの装置は、取り付けられたスピーカまたはヘッドフォン132を有するか、あるいは外部増幅器およびスピーカ、カセット・アダプタなどのオーディオ再生機器に入力するのに適したアナログ・オーディオ出力を有する音声回路130である。音声回路130は、オーディオ・ファイルを再生する技術分野でよく知られている。別法として、音声回路は、オーディオ・データを無線受信機によって受信され再生されるように予め決められている周波数上で送信する無線送信機でよい。他の無線方法も可能である。

【0009】

図1に示すシステムの任意の構成要素またはすべての構成要素および関連するハードウェアを本発明の様々な実施形態で使用できることに留意されたい。しかし、当業者には、システムの任意の構成を特定の実装による様々な目的に使用できることが理解されよう。本発明の一実施形態では、図1に示すデータ処理システムはIBM（登録商標）互換パソコン・コンピュータ（PC）、Apple Macintosh（登録商標）パソコン・コンピュータ、またはSUN（登録商標）SPARC Workstationである。プロセッサ102は、Santa Clara, CaliforniaのINTEL（登録商標）Corporationによって製造されている80486またはPENTIUM（登録商標）ブランド・マイクロプロセッサなどの80×86互換マイクロプロセッサのうちの1つでよい。

【0010】

本発明を実現するソフトウェアは、メイン・メモリ104、大容量記憶装置107、またはプロセッサ102からアクセスできるその他の記憶媒体に記憶することができる。当業者には、本明細書で説明する方法およびプロセスを、メイン・メモリ104または読み取り専用メモリ106に記憶されプロセッサ102によって実行されるソフトウェアとして実現できることが明らかになろう。このソフ

トウェアは、コンピュータ可読プログラム・コードを有するコンピュータ使用可能大容量記憶媒体108を備える製品上に存在することもでき、コンピュータ可読プログラム・コードは、コンピュータ使用可能大容量記憶媒体内に実装され、大容量記憶装置107によって読み取ることができ、プロセッサに本明細書の教示に従ってデジタル情報ライブラリ・トランザクションおよびプロトコルを実行させることができる。

【0011】

デジタル情報ライブラリ・システム

図2は、本発明の好ましい実施形態で使用されるコンピュータ・ネットワーク・アーキテクチャを示す。一般に、本発明のネットワーク・アーキテクチャは、従来型の配信網インフラストラクチャ240を介してクライアント・サイト210に結合されたライブラリ・サイト250を含む。この従来型の配信網インフラストラクチャ240は、インターネット・プロバイダを介してライブラリ・サイト250とクライアント・サイト210との間に設けられる標準電話接続として実現することができ、従来型の電話網を介したインターネット上のデータ通信を可能にする。このようなインターネットの配信網としての使用法は、当業者によく知られている。ケーブル・モ뎀機能を有する代替実施形態では、電話網を介した通信の代わりに従来型のケーブル網を介した通信が可能である。ケーブル網は通常、標準電話網よりもずっと高速である（すなわち、ずっと大きな帯域幅を与える）。しかし、ケーブル・モ뎀は標準POTS（単純な在来型電話サービス）モ뎀よりも高価である。従来型の総合サービス・デジタル網（ISDN）機能を有する他の代替実施形態では、配信網240はISDNモ뎀を使用してアクセスされる。この場合も、ISDN網は通常、POTS網よりも高速である。しかし、ISDN網へのアクセスは一般に、より費用がかかる。ケーブル・モ뎀およびISDN実装は、POTS実装の代替通信媒体である。

【0012】

また、当業者には、他の形態のネットワーク化を本発明によって同様にサポートできることが明らかになろう。たとえば、赤外線リンクや無線リンクなどの無線送信手段も、本出願で説明する配信網240を形成することができる。インタ

一ネットの代替策として、AMERICA-ON-LINE (AOL) やCOMPU-SERVEなど独自のネットワーク／掲示板を使用することができる。

【0013】

ライブラリ・サイト250の各サーバおよびクライアント・サイト210のクライアント・コンピュータ・システム214は、上記で図1に関連して説明したようなコンピュータ・システムとして実現することができる。当業者には、前述の技法を使用して、ライブラリ・サーバ260、オーサリング・システム280、および認証サーバ270をリモートに配置し、しかも配信網としてネットワーク化できることが明らかになろう。また、本発明では、複数のライブラリ・サーバ、オーサリング・システム、および認証サーバを使用することができる。逆に、サーバを単一のマシンの独立の機能として実現することができる。これらの代替実施形態について、図4ないし図8に示し、以下に詳しく説明する。

【0014】

移動再生装置212は、最小限の構成を有する低コストの独立式移動ユニットであり、ライブラリ・サーバ260およびクライアント・コンピュータ・システム214によってダウンロードされたデジタル情報ファイルまたはプログラムを受信して記憶し、移動再生装置212のユーザ用のデジタル情報ファイルまたはプログラムを再生する。移動再生装置212は、ダウンロードが行われている間にクライアント・コンピュータ・システム214に一時的に着脱可能に結合される。ダウンロード後、移動再生装置212をクライアント・コンピュータ・システム214から取り外し、独立式デジタル情報再生装置として使用することができる。「Interactive Audio Transmission, Receiving and Playback System」(米国特許出願第08/490,537号)と題し、Montclair, NJのAudible Words Corporationに譲渡されたする関連米国特許出願は、移動再生装置212の詳細を説明している。

【0015】

本発明の好ましい実施形態は、その基本形態では、コンピュータ・ネットワークを介して必要に応じてデジタル情報プログラミングの選択を可能にするデジタ

ル情報ライブラリ・システムである。代替実施形態では、デジタル情報プログラミングがコンピュータ・ネットワークを介して選択されるが、大容量記憶媒体241を使用して供給される。この代替実施形態について以下に詳しく説明する。

【0016】

このデジタル情報ライブラリは、デジタル情報プログラミング、書籍や毎日のニュースやエンターテインメント・フィーズなどのデジタル情報源から得た描画コンテンツ、会議および教育情報源、他のコンピュータ・システム、インターネットのワールド・ワイド・ウェブ(WWW)上のホスト、ならびにカスタマイズされたオーディオまたはビジュアル画像プログラミングのインデックス付き集合である。他のデジタル情報コンテンツ源には、会議またはセミナーの議事録、講義またはスピーチの資料、言語レッスン、読物、コメディー、カスタマイズされたスピークン・ダイジェスト、および関連する「必須」ビジネス情報、コンピュータ・ソフトウェア、ローカル・サウンド・スタジオ・マテリアル、機械可読ファイルのテキスト・スピーチ変換、磁気テープから得られる記録済みのマテリアル、CD-ROM、デジタル・オーディオ・テープ、またはアナログ・カセット・テープが含まれるが、これらに限らない。このデジタル情報コンテンツは、図2に示すオーサリング・システム280への生デジタル情報コンテンツとして入力される。代替実施形態では、生入力を受信し、この入力をデジタル形式に変換する生デジタル情報デジタイザ307が含まれられ、このデジタル形式をデジタル情報ファイルとして処理することができる。

【0017】

代替実施形態では、デジタル情報は、表示画面または投影画面上でビジュアル画像を生成するために使用されるデジタル化画像またはグラフィックス・データを含む。これらの画像は、ライブラリ・サーバ260によって保持され、維持されるデジタル情報に含めることもできる。

【0018】

オーサリング・システム

オーサリング・システム280は、デジタル情報コンテンツを編集し、インデックス付けし、圧縮し、スクランブルし、セグメント化し、カタログ化してデジ

タル情報ファイル内のデジタル情報プログラムを得るために使用され、このデジタル情報プログラムは、大容量記憶媒体241上に記憶されるか、あるいはスクランブルされ圧縮されたデジタル情報ファイル262としてライブラリ・サーバ260上に記憶される。デジタル情報プログラムは最初、従来型の基準（たとえば、ジャンル、現代フィクション、ミステリー、アドベンチャー、ロマンス、ノンフィクション、クラシック、セルフヘルプ、サイエンス・フィクション、ウェスタンなど）に従って分類される。特定の著者または発行者に関連する範疇も与えられる。完全なタイトルと短縮タイトルの両方が与えられる。いくつかの状況では、デジタル情報コンテンツを非デジタル化形式からデジタル化する必要がある。この目的のために生情報デジタイザ307が用意されている。オーサリング・システム280はまた、デジタル情報コンテンツをセグメントに区画し、これらのセグメントを必要に応じて識別し、探索し、スキップすることができる。すべてのこれらの機能はオーサリング・システム280によって実行される。

【0019】

図3は、好ましい実施形態のオーサリング・システム280を示す。オーサリング・システム280は、デジタル情報コンテンツを様々な従来型の情報源から生デジタル化データとして受信する。このデジタル情報データは、好ましい実施形態のオーサリング・システム280の3つの構成要素に供給される。デジタル情報コンプレッサ314は、生デジタル・データを受信し、デジタル化データを圧縮する。デジタル・データを圧縮する様々な従来型の技法が存在する。これらの技法は、処理されるデジタル・データの種類に応じて最適化することができる。したがって、本発明は、いくつかの圧縮方法と、オーサリング・システム・オペレータ305が、デジタル情報コンプレッサ314に入力されるデジタル情報コンテンツ310の範疇に基づいてこれらの方法のうちの1つを選択できるようにする手段とを提供する。別法として、圧縮方法の選択は、デジタル情報コンテンツ310自体を解釈することによって自動的に実行することができる。圧縮されたデジタル情報ファイルはデジタル情報コンプレッサ314によってスクランブラー318に出力される。

【0020】

生デジタル情報コンテンツ 310 はテンプレート・ヘッダ生成装置 312 にも供給される。ライブラリ・サーバ 260 によって維持される各デジタル情報ファイルは、ファイルのコンテンツを識別するために使用されると共に、ファイル内のデジタル情報を処理するために使用される情報を与えるために使用される他の記述的情報を含む。各デジタル情報ファイルは、テンプレート・ヘッダ、スクランブル解除マップ、選択されたプレビュー・クリップ、およびデジタル情報プログラミング自体を含む。好ましい従来型では、テンプレート・ヘッダは、ファイル内のデジタル情報に対応するいくつかの属性を含む。たとえば、デジタル情報は、書籍または発行された他の作品のコンテンツから生成されるオーディオ情報でよい。この例では、オーディオ・ファイル・テンプレート・ヘッダは、1) 書籍のタイトル、巻、またはデジタル情報コンテンツを得た媒体、2) デジタル情報コンテンツに関する著作権、3) コンテンツの可聴タイトル、4) コンテンツの目次、および5) デジタル情報を適切に再生またはレンダリングするための再生設定を含む属性を含む。目次は、章の数、プログラムの長さ、および関連コンテンツ・セクションを示す情報を含むがこれらに限らないコンテンツ・ナビゲーション情報を含む。目次は、オーサリング・システム・オペレータ 305 からの入力を用いて生成されるか、あるいはデジタル情報コンテンツ 310 を分析することによって自動的に生成される。スクランブル解除マップ 322 は、後述のようにスクランブル 318 によってデジタル情報がスクランブルされた後でデジタル情報を解釈するために使用される。プレビュー・クリップ 324 は、特定のデジタル情報ファイルのコンテンツの概略を消費者に示すために使用されるデジタル情報コンテンツの事前に生成された短い部分を含む。好ましい実施形態では、このようなプレビューは、音声生成回路 130 によって直接再生するか、あるいは他の手段によってレンダリングすることのできる従来型のフォーマット済みファイルとして生成される。デジタル情報ファイルにはいくつかのプレビュー・クリップ 324 は圧縮されることもあるいはスクランブルされることもない。テンプレート・ヘッダ 312 は、ネットワーク 240 または大容量記憶媒体 241 に転送される際にデジタル情報ファイルを保持する。デジタル情報ファイル用の他の

記述的情報は通常、デジタル情報ファイルと共に記憶されるが、そのように記憶する必要はない。

【0021】

再び図3を参照するとわかるように、テンプレート・ヘッダ生成装置312は、デジタル情報コンテンツ310の特定の部分からテンプレート・ヘッダを生成する。ヘッダ生成プロセス中にオーサリング・システム・オペレータ305およびデジタル情報コンプレッサ314からの入力を要求することができる。テンプレート・ヘッダはライブラリ・サーバ260に与えられる。デジタル情報ファイル・ヘッダの他の部分はスクランプラ318およびプレビュー生成装置323から与えられる。デジタル情報ファイル・ヘッダのこれらの部分は、ライブラリ・サーバ260によってアセンブルされ、特定のデジタル情報ファイル用のヘッダが得られる。デジタル情報ファイルの残りの部分には、圧縮されスクランブルされセグメント化されたデジタル情報コンテンツが満たされる。

【0022】

デジタル情報コンプレッサ314が、デジタル情報の範疇に適した選択された圧縮方法を使用して生デジタル情報を圧縮した後、スクランプラ318がデジタル情報をスクランブルする。デジタル情報は、許可されていない消費者がこのデジタル情報を使用するのを防止するためにスクランブルされる。好ましい実施形態では、スクランプラ318は従来型の暗号化方法を使用してデータを使用不能にする。スクランブルされたデジタル情報ファイルをスクランブル解除する手段となる、対応するスクランブル解除マップ322が生成される。スクランプリング・マップ316は、デジタル情報ファイルをスクランブルするためにスクランプラ318によって使用される。スクランプラ318は、デジタル情報ファイル全体、またはデジタル情報ファイルの選択された重大なサブセットを暗号化することができる。スクランプリングのレベルは、オーサリング・システム280、移動再生装置212、および／またはクライアント・コンピュータ・システム214上の予想されるソフトウェア・プレーヤー226の機能に応じて選択することができる。代替実施形態では、スクランプラ318の代わりに独自のデジタル情報フォーマットが使用される。

【0023】

スクランブルされたデジタル情報コンテンツは、スクランブル318によってセグメント化論理326に出力される。セグメント化論理326は、デジタル情報コンテンツを、移動再生装置212またはソフトウェア・プレーヤー226に効率的に記憶されかつ転送され、かつ再生中に効率的にナビゲートされるブロックに区画する。トランスポート完全性データが生成され、セグメント化されたデジタル情報に付加される。代替実施形態では、セグメント化プロセスの一部をデジタル情報コンプレッサ314およびスクランブル318の前または後に行うことができる。テンプレート・ヘッダ生成装置312によって、ヘッダ生成プロセスでセグメント化情報を使用することができる。圧縮され、スクランブルされ、セグメント化されたデジタル情報ブロックは、オーサリング・システム280によってライブラリ・サーバ260に与えられる。ライブラリ・サーバ260は、デジタル情報コンテンツの特定のアイテムに関するセグメント化されたデジタル情報ブロック、スクランブル解除マップ322、プレビュー・クリップ324、およびテンプレート・ヘッダ312をアセンブルしてデジタル情報プログラム・ファイルを得る。このデジタル情報プログラム・ファイルはデジタル情報プログラム・ファイル記憶領域262に記憶される。他の生デジタル情報コンテンツは、オーサリング・システム280を同様に使用してデジタル情報ファイルに変換される。

【0024】

ライブラリ・サーバ

再び図2を参照する。ライブラリ・サーバ260は、オーサリング・システム280によって作成されたデジタル情報プログラム・ファイル262を維持する責任を負う。また、ライブラリ・サーバ260は、ネットワーク240を介したクライアント・コンピュータ・システム214からデジタル情報プログラム・ファイル262へのアクセスを求める要求を受信し、選択されたデジタル情報ファイルの購入および供給ならびに／または選択されたプレビュー・クリップ324の供給を管理する。ライブラリ・サーバ260は、これらのライブラリ・サーバ機能と、後述の認証プロトコルに使用されるライブラリ・キー263とを実行す

るライプラリ管理ソフトウェア 261 を含む。ライプラリ管理ソフトウェア 261 は、デジタル情報プログラム・ファイル 262 のアクセスおよび／または購入を求めるクライアント・コンピュータ・システム 214 の要求を受信し、これに応答する処理論理を含む。ライプラリ・サーバ 260 は、このようなクライアント要求を受信した後、認証サーバ 270 を使用して、ライプラリ・サーバ 260 または認証サーバ 270 によって生成され維持されるクライアント情報 272 を用いてこの要求を認証する。クライアント情報 272 にはクライアント識別子が含まれ、クライアント識別子は、コンテンツを、個々の移動再生装置 212 またはソフトウェア・プレーヤー 226 上で再生されるようにターゲティングするために使用される。クライアント情報 272 には、クライアント個人情報、ユーザ・コンテンツ優先順位、クライアント課金履歴、プレーヤー使用履歴、およびプレーヤー・グループ・リストを含めることができる。代替実施形態では、この代わりにクライアント情報 272 の一部をサーバ 260 に記憶することができる。

ライプラリ・サーバ 260 は、以下に詳しく説明する認証プロトコルを使用して、クライアント要求を満たすことができるかどうかを判定する。承認された場合、ライプラリ・サーバ 260 は、クライアント・コンピュータ・システム 214 によって要求されたデジタル情報プログラム・ファイルまたはレビュー・クリップにアクセスし、選択されたレビュー・クリップを供給するか、あるいは以下に詳しく説明する認証プロトコルを使用して暗号化され、ターゲティングされたデジタル署名付きデジタル情報ファイルを構築し、暗号化され、圧縮されたデジタル情報ファイルをネットワーク 240 を介して要求側クライアント・コンピュータ・システム 214 に転送する。クライアント・システム 214 に情報を転送する供給媒体として配信可能な大容量記憶媒体 241 を使用することもできる。この場合、クライアント・コンピュータ・システム 214 は、選択されたデジタル情報ファイル（またはそのサブセット）を後で再生できるように移動再生装置 212 に独立にダウンロードすることができる。ライプラリ・サーバ 260 はまた、デジタル情報ファイル 262 のアクセス履歴に関する使用状況統計を収集し、この使用状況データを使用状況統計記憶領域 264 に記憶する。ライプラリ・サーバ 260 は、クライアント・ブラウザ 219、ソフトウェア・プレーヤー

226、および移動再生装置212用の命令コード・セグメント（フォームウェア）も記憶する。この命令コードは、デジタル情報ファイルを転送する場合と同様にクライアント・コンピュータ・システム214にダウンロードすることができる。再生装置212およびソフトウェア・プレーヤー226に関するプレーヤー構成データは、ライブラリ・サーバ260上に記憶され、デジタル情報ファイルおよびファームウェアを転送する場合と同様にカスタマイズまたは更新することができる。構成データには、オーディオ・プロンプト、ユーザ・インターフェース・オプション、グループID情報、および情報再生パラメータが含まれるが、これらに限らない。プレーヤー構成データは、クライアント情報272の必要に応じてクライアント・コンピュータ・システム214、ソフトウェア・プレーヤー226、または移動再生装置212に転送される。

【0025】

ライブラリ・サーバ260は、クライアント・コンピュータ・システム214で実行されるクライアント・アプリケーション・プログラムまたはクライアント・プラウザ219とのインターフェースをとる。クライアント・プラウザ219は、デジタル情報ファイル262での所望のプログラムの探索、デジタル情報ファイル262に関連する選択されたプレビュー・クリップの確認、選択されたプログラムの購入、命令コード・セグメントまたはプレーヤー構成データの要求、購入されたプログラムまたはその他のマテリアルの要求側クライアント・コンピュータ・システム214へのダウンロードを含むが、これらに限らない様々な種類のサービスをライブラリ・サーバ260に要求するために使用される。

【0026】

ライブラリ・サーバ260は認証サーバ270とのインターフェースをとり、クライアント・コンピュータ・システム214は、本発明の好ましい実施形態の固有の認証プロトコルおよび暗号化プロトコルを使用する。これらのプロトコルの好ましい実施形態について以下の節で説明する。

【0027】

クライアント・コンピュータ・システム

再び図2を参照するとわかるように、クライアント・コンピュータ・システム

214は、消費者コンピュータ・システムまたはエンド・ユーザ・コンピュータ・システム、通常は、図1に示すサンプル・システムなどのパーソナル・コンピュータを表す。消費者は、このパーソナル・コンピュータを用いて、配信網240を介してデジタル情報ライブラリ・サーバ260のデジタル情報コンテンツをブラウズし、確認し、選択し、購入し、供給させることができる。クライアント・コンピュータ・システム214は、クライアント・ブラウザ・ソフトウェア219と、移動装置インターフェース221と、ネットワーク240からダウンロードされた暗号化され圧縮されたデジタル情報ファイル220用の記憶域と、ソフトウェア・プレーヤー226と、移動再生装置212内の記憶セグメントを決め、デジタル情報ファイル220のクライアント・コンピュータ・システム214から移動再生装置212へのダウンロードを助ける、デジタル情報ファイル220から得られるセグメント・ダウンロード・データ222とを備える。クライアント・コンピュータ・システム214は、サーバ260から受信されたデジタル情報およびソフトウェア・ファイルを認証するために使用されるサーバ公開鍵215も含む。クライアント・ブラウザ・ソフトウェア219は、クライアントまたは消費者が、ライブラリ・サーバ260のデジタル情報ライブラリ262にアクセスしタイトルを購入するために用いる制御論理を実現する。クライアント・ブラウザ・ソフトウェア219は、サーバ260に構成情報または命令コードを要求し、それらをダウンロードする制御論理も実現する。クライアント・ブラウザ・ソフトウェア219は、直接的な人間の介入なしにこれらの動作を実行するよう構成することができる。移動装置インターフェース221は、クライアント・コンピュータ・システム214から移動再生装置212への、制御情報、命令コード、及びデジタル情報ファイルの転送を制御するために使用されるソフトウェア・インターフェースである。暗号化され圧縮されたデジタル情報ファイル220は、クライアント・コンピュータ・システム214によって、ネットワーク240を介してライブラリ・サーバ260から受信される。代替実施形態では、ネットワーク240ではなく配信可能な大容量記憶媒体241を使用してクライアント・コンピュータ・システム214に情報を転送する。ソフトウェア・プレーヤー226は、移動再生装置212の動作をエミュレートすると共に、クライア

ント・コンピュータ・システム214の音声回路130およびオーディオ出力装置132を通してデジタル情報ファイルを再生するために使用されるソフトウェア・モジュールである。ソフトウェア・プレーヤー226用の命令コードおよび構成情報は、移動再生装置212のダウンロードまたは更新を行う場合と同様にサーバ260からダウンロードし更新することができる。ソフトウェア・プレーヤー226機能は、移動再生装置212の機能および動作に相当する。したがって、本明細書全体にわたって使用される「プレーヤー」の語は一般に、移動再生装置212とソフトウェア・プレーヤー226の両方に当てはまる。ソフトウェア・プレーヤー226には固有のプレーヤーIDが割り当てられ、かつ移動再生装置212に割り当たるIDと同様に機能するグループIDを割り当てることができる。

【0028】

移動再生装置

移動再生装置212は、デジタル情報ファイルを、オーディオ出力手段を通して再生される音声、または表示装置上に表示される表示可能な画像に変換する。好ましい実施形態では、移動再生装置212は、最小限の機能を有する低コストの装置であり、主としてオーディオ・ファイルの再生またはビジュアル画像またはテキストの表示装置上への表示専用に使用される。移動再生装置212は、軽量で低コストで容易に移動可能な特徴を保持するように最小限の構成を有する。したがって、好ましい実施形態では、ポータブル・パーソナル・コンピュータやラップトップ・コンピュータを移動再生装置212として使用することはない。というのは、このような汎用コンピューティング装置は通常、好ましい移動再生装置212の軽量制約および低コスト制約を満たさないからである。このような汎用コンピューティング装置は通常、不要な機能と複雑なインターフェースを有し、専用移動再生装置212と比べてコストおよび性能面の欠点を有することがある。好ましい実施形態では、移動再生装置212は、プロセッサ、メモリ、およびクライアント・コンピュータ・システム214とのインターフェースを含み、このインターフェースを介して圧縮デジタル情報ファイル216が受信される。以下に詳しく説明するように、移動再生装置212は、クライアント・コンピュータ

・システム 214 を介してサーバ 260 から受信されたデジタル情報およびソフトウェア・ファイルを認証するために使用されるプレーヤー ID 223、グループ ID 225、およびサーバ公開鍵 215 も含む。ユーザは、装置上に設けられたボタンおよびノブを使用して移動再生装置 212 を制御する。これらの制御装置は、デジタル情報ファイル 216 をナビゲートするか、構成データおよび再生パラメータを調整するか、あるいは再生装置 212 に記憶されているファームウェアの指示に応じて他の機能を実行するために使用される。クライアント・コンピュータ・システム 214 あるいは他の電子装置は、プレーヤーに結合されると、これらの制御装置からのユーザ入力を要求することができる。代替実施形態では、有線接続または無線接続を介してプレーヤーに結合されたリモート制御ユニット上に 1 組の追加のユーザ制御装置が設けられる。ヘッドフォン・ジャックを介すか、あるいはボード・スピーカまたは無線送信機上で、スピーカまたはヘッドフォンを有する独立の無線受信機にデジタル情報出力を与えることができる。オーディオ・レベルはボリューム・ノブを用いて調整することができる。無線送信機は、送信周波数またはその他の送信パラメータを調整する調整ノブを含むことができる。ビジュアル情報出力は、LCD ディスプレイまたは LED ディスプレイを介して与えられるか、あるいは標準ビジュアル表示装置への出力を介して与えられる。移動再生装置 212 は、限られた量の非揮発性メモリ、RAM、および ROM を含む。デジタル情報コンテンツ、構成データ、および命令コードは移動再生装置 212 のメモリ空間に記憶される。構成データには、パブリック ID およびプライベート ID、コンテンツ再生パラメータ、およびユーザ・インターフェース・パラメータが含まれるが、これらに限らない。非揮発性メモリを使用することによって、デジタル情報コンテンツ、構成データ、およびファームウェアの一部をダウンロードを介して更新することができる。デジタル情報コンテンツとファームウェア（オペレーティング・ソフトウェア）は共に、このメモリ装置に記憶される。ファームウェアおよび構成情報の一部は永久的に読み取り専用メモリ（ROM）に記憶される。移動再生装置 212 のメモリのコンテンツを追跡するために内部メモリ割付け方法が使用される。この割付け方法は、セグメント・ナビゲーション・データ 218 と共に、移動再生装置 212 メモリに存在する

所望のデジタル情報、プログラム、構成データ、またはヘッダ・データを見つける手段も実現する。移動再生装置212はクライアント・コンピュータ・システム214とのインターフェースを含み、このインターフェースを介して、圧縮デジタル情報ファイル216、ソフトウェアの更新、および構成の変更をクライアント・コンピュータ・システム214から受信する。

【0029】

デジタル情報コンテンツ、ソフトウェアの更新、または構成情報の、ライブラリ・サーバからクライアント・コンピュータ・システムへのダウンロード
クライアント・コンピュータ・システム214のクライアント・ブラウザ・ソフトウェア219は、ライブラリ・サーバ260のライブラリ管理ソフトウェア261、および移動再生装置212に存在するファームウェアと協働し、消費者が配信網240を介してデジタル情報ライブラリ・サーバ260のデジタル情報コンテンツをブラウズし、確認し、選択し、選択したデジタル情報コンテンツを購入し、供給させることができる手段を実現する。デジタル情報コンテンツは通常、購入時にクライアント・コンピュータ・システム214にダウンロードされるが、1) 購入後のある時点で、あるいは2) 最初の購入後の複数の時点で、デジタル情報コンテンツをダウンロードすることが可能である。クライアント・ブラウザ219は、ユーザの介入なしにクライアント・コンピュータ・システム214にコンテンツをダウンロードするように構成することができる。また、クライアント・コンピュータ・システム214ソフトウェア自体の一部または移動再生装置212常駐ソフトウェア／ファームウェアの一部をライブラリ・サーバ260からダウンロードまたは更新することができる。移動再生装置212に常駐するソフトウェア／ファームウェアはクライアント・コンピュータ・システム214を介してダウンロードされる。ライブラリ・サーバ260が、クライアント・コンピュータ・システム214ソフトウェアまたは移動再生装置212のソフトウェア／ファームウェアの更新済みコピーまたはより新しいコピーを有する場合、このライブラリ・サーバ・コピーがダウンロードされ、対応するクライアント・コンピュータ・システム214のソフトウェアまたは移動再生装置ソフトウェア212の古いバージョンに取って代わる。ソフトウェアは、デジタル情報フ

ファイルのスクランブリングおよび供給の場合と同様に暗号化され、スクランブルされ、デジタルに署名される。再生装置 212 用の ID リスト、オーディオ・プロンプト、およびその他の構成データに対する変更は、ライブラリ・サーバ 260 からソフトウェアの更新をダウンロードする場合と同様にダウンロードすることができる。

【0030】

好ましい実施形態は、認証プロセスを使用してサーバ 260 からクライアント・システム 214 および再生装置 212 への情報の転送を保護する。第 1 に、ポイント・ツー・ポイント認証プロトコルが実行され、そのため、ライブラリ・サーバ 260 は、要求側クライアント・コンピュータ・システムが許可されたクライアントであることを検証しなければならず、クライアント・コンピュータ・システム 214 は、ライブラリ・サーバ 260 が許可されたプロバイダであることを検証しなければならない。第 2 に、ターゲティング・プロトコルが実行され、そのため、ライブラリ・サーバ 260 は、選択されたダウンロード・データをライブラリ・サーバ 260 から受信することを許可された移動再生装置 212 に 1 組の識別子（すなわち、プレーヤー ID）を使用する。移動再生装置識別子は、クライアント・コンピュータ・システム 214 から与えられるか、あるいはライブラリ・サーバ 260 上に記憶されているユーザ・プロファイルから参照される。ターゲティング・プロセスで、ライブラリ・サーバ 260 は、移動装置 212 によってこのような識別子を用いないかぎり読み取ることもあるいは再生するともできないデータをフォーマットしダウンロードする。第 3 に、ダウンロードされたデータが許可されたライブラリ・サーバから発振されたデータであることを検証すると共に、ダウンロードされたデータの完全性を検証するために、移動再生装置 212 によって使用されるライブラリ・サーバ・デジタル署名が、ダウンロードされたデータに付加される。本発明のこの 3 つの認証プロセスについて以下に詳しく説明する。

【0031】

ポイント・ツー・ポイント認証プロトコル
ライブラリ・サーバ 260、クライアント・コンピュータ・システム 214、

および移動再生装置212はそれぞれ、他のシステムの真正さを検証するために使用される固有の検証シーケンスを有する。ライブラリ・サーバ260とクライアント・システム214との間の通信で、2つのシステムは交互に、(1)他のシステムの検証を要求し、(2)検証要求に対する認証応答を与えるように動作する。移動装置212とクライアント・コンピュータ・システム214との間の通信では、同様な認証プロトコルが使用されると共に、クライアント・システム214を介した移動装置212とライブラリ・サーバ260との間のリアルタイム通信が使用される。この検証シーケンスは、事前に決められている1組のビット・ストリームまたはデータ構造を含み、これらのビット・ストリームまたはデータ構造は、ポイント・ツー・ポイント送信で認証されている受信側システム(すなわち、受信側)に要求側システム(すなわち、検証を要求しているシステム)から送信される。受信側システムは、特定の応答ビット・ストリームまたはデータ構造を要求側システムに送信することによって、予め決められている方法で検証シーケンスに応答しなければならない。応答側からの適切な応答データが要求側システムによって受信された場合、検証中のシステムは、許可されたシステムとみられる。逆に、予め決められているタイムアウト期間が満了する前に、要求側システムによって適切な応答データが受信されなかった場合、検証中のシステムは許可されていないとみられる。2つのシステムは、別々の検証サイクルで要求側および応答側として働くことによって通信を開始する。これらのポイント・ツー・ポイント認証サイクルが完了した後、両方のシステムが互いを許可されたシステムであると判断した場合にのみ、さらなるクライアント/サーバ処理が継続する。

【0032】

代替実施形態では、ライブラリ・サーバ260、クライアント・コンピュータ・システム214、および移動再生装置212の間の通信サブセットでポイント・ツー・ポイント認証が使用される。他の実施形態では、ポイント・ツー・ポイント認証は使用されず、システム・セキュリティはターゲティングおよび/またはデジタル署名認証の使用に依存する。

【0033】

ターゲティング・プロトコル

本発明のターゲティング・プロトコルは、デジタル情報コンテンツの再生、プレーヤー構成データの調整、および指定されたプレーヤー 212/226 または指定された 1 組の移動再生装置 212 へのプレーヤー命令コードのダウンロードを制限する手段および方法である。各プレーヤー 212/226 は固有のプレーヤー ID 223 を含む。プレーヤー ID 223 はパブリック・プレーヤー ID およびプライベート・プレーヤー ID を含む。パブリック・プレーヤー ID は固有の識別子であり、プレーヤーを識別するための通し番号として働く。プライベート・プレーヤー ID は、個々の移動再生装置 212 用のデータをターゲティングするために使用される。インストール中を除いて、プライベート・プレーヤー ID が通信リンクやネットワーク・パスを介して送信されることはない。好ましい実施形態では、各プライベート・プレーヤー ID は十分に離散すべきであるが、固有の ID である必要はない。

【0034】

移動再生装置 212 は、グループ ID を使用して論理的にグループ分けすることができる。デジタル情報コンテンツ、ソフトウェア、または構成データは、グループ ID によって決まる 1 群の移動再生装置 212 をターゲティングすることができる。各プレーヤー 212/226 は、特定のプレーヤー 212/226 がメンバーである 1 つまたは複数のグループ ID 225 を記憶するためのメモリ空間を含む。各グループ ID はパブリック部およびプライベート部を含み、これらの部分はそれぞれ、パブリック・プレーヤー ID およびプライベート・プレーヤー ID に相当する。各グループは、他のプレーヤー ID やグループ ID と共用されない固有の値のパブリック ID によって識別される。デジタル情報コンテンツ、ソフトウェア、または構成データは、特定のプレーヤー ID のターゲティングの場合と同様に特定のグループ ID をターゲティングすることができる。同じグループ内の移動再生装置 212 は同じグループ ID を共用する。特定のグループ ID は、すべての移動再生装置 212 がメンバーであるグローバル・グループとして事前に決められる。移動再生装置 212 は、複数のグループのメンバーでよい。特定のプレーヤー 212/226 に維持されている 1 組のグループ ID に新

しいグループIDを付加することによって、特定のプレーヤー212/226が新しいグループに追加される。この新しいグループIDは、サーバ260がパブリック・グループIDおよびグループ鍵をクライアント・コンピュータ・システム214を介してプレーヤー212/226に与えた後で付加される。プレーヤー212/226は、グループ鍵と移動再生装置212のプライベート・プレーヤーIDとの組合せからプライベート・グループIDを生成する。プライベート・プレーヤーIDの場合と同様に、インストール中を除いて、プライベート・グループIDが通信リンクやネットワーク・パスを介して送信されることはない。

代替実施形態では、プレーヤーは、グループ・プライベートIDを直接、あるいはグループ鍵をプレーヤー・パブリックIDまたは他の既知の数値と組み合わせることによって受信する。他の代替実施形態では、プライベート・グループIDは、ターゲティング・プロセスでは使用されず、プレーヤーには転送されない。

グループ割当てプロセスは、クライアント・システム214を介してサーバ260とプレーヤーとの間でリアルタイム通信を使用することに制限するか、あるいはグループ割当がクライアント・システム214にダウンロードされた後のある時点で行うことができる。本発明で決められるプレーヤーIDおよびグループIDについて説明したが、次にターゲティング・プロトコルにおけるこれらのIDの使用法について説明する。

【0035】

ライブラリ・サーバ260は、図2に示すプレーヤーIDテーブル266を含む。プレーヤーIDテーブル266は、プライベートIDおよびパブリックID用の記憶領域を含む。プライベートIDは、新しい移動再生装置がシステムにインストールされたときか、あるいは新しいグループが確立されたときにプレーヤー・テーブル266にプリロードされる。他の実施形態では、IDテーブル266は数学的関数であり、グループ・パブリックIDまたはプレーヤー・パブリックIDを変換する。クライアント・コンピュータ・システム214が特定のプレーヤー212/226または1組の移動再生装置212を特定の指定されたデジタル情報、ソフトウェア・コンテンツ、または選択された構成データにターゲティングする必要があるときに、クライアント・コンピュータ・システム214に

よってパブリック・プレーヤー ID およびパブリック・グループ ID がサーバ 260 に送信される。デジタル情報の選択は、ライブラリ・サーバ 260 上に記憶されているファイル 262 から行われる。ソフトウェアまたは構成データの選択は、サーバ 260 上に記憶されているファイル、またはサーバ 260 による要求に応じて生成されるデータから行われる。ソフトウェア・コンテントおよび構成データは、デジタル情報コンテンツに対するオーサリング・プロセスと同様に作成されスクランブルされる。クライアント・コンピュータ・システム 214 によって 1 組のターゲティングされたパブリック ID とサーバ 260 から転送すべき関連データとが関連付けされた後、ライブラリ・サーバ 260 は、選択されたファイルのターゲティングされたヘッダを作成する。ライブラリ管理ソフトウェア 261 は、パブリック ID 一プライベート ID テーブル 266 を参照し、対応するターゲティングされたプライベート ID を見つける。ターゲティングされたヘッダは、選択されたファイルから得られるスクランブル解除マップ 322 と、ターゲティングされた移動再生装置 212 に対応するプライベート・プレーヤー ID との組合せを含む。したがって、ターゲティングされた移動再生装置 212 の秘密 ID を使用してスクランブル解除マップ 322 が暗号化される。ターゲティングされたこのヘッダは、ネットワーク・トранSPORT・レディ・データ・ブロック内の選択されたファイルの対応するデジタル情報またはソフトウェア・コンテントとリンクされる。以下にデータ署名プロトコルに関連して説明するよう にこのデータ・ブロックにデジタル署名が適用される。このデータ・ブロックにトランSPORT 完全性データ（チェックサムまたは循環冗長検査の使用など）が適用され、データ・ブロックはネットワーク 240 を介してクライアント・コンピュータ・システム 214 に送信される。対応するスクランブル解除ブロック 322 をデータ・ブロックのヘッダで使用しないかぎりデータ・ブロックをスクランブル解除することはできず、かつスクランブル解除ブロック 322 が、ターゲティングされた移動再生装置 212 しか知らないプライベート ID と組み合わされている（すなわち、暗号化されている）ので、このデータ・ブロックをスクランブル解除し読み取ることのできるのは、ターゲティングされた移動再生装置 212だけである。したがって、選択されたデジタル情報、ソフトウェア・コンテ

ント、および構成データは、特定の1組の移動再生装置212にターゲティングされる。

【0036】

小さな移動再生装置212群の場合、デジタル情報ファイルのターゲティングされた各ヘッダは複数のスクランブル解除マップを含むことができ、各スクランブル解除マップは異なるプレーヤー212／226に関連付けられる。このように、複数の移動再生装置212は、クライアント・コンピュータ・システム214上に記憶されている単一のファイル220を読み取ることができる。

【0037】

当業者は、代替ターゲティング方法が存在することに留意されたい。代替実施形態では、ライプラリ・サーバ260は、ターゲティングされた受信側のプライベート・プレーヤー212／226識別子またはターゲティングされたグループのプライベート・グループ識別子を使用してスクランブル・マップ316を生成する。スクランブル解除マップ322は、受信側プレーヤーまたは受信側グループによってすでに知られているのでファイルと共に記憶されることはない。この方法では、単一のプレーヤー212／226またはグループにコンテンツがターゲティングされ、コンテンツの許可されない再生を防止する場合と同一の結果が達成される。

【0038】

他の代替実施形態では、ライプラリ・サーバ260はデジタル情報コンテンツをスクランブルすることも、あるいは既知の鍵を使用してデジタル情報コンテンツをスクランブルすることもない。この実施形態では、スクランブル解除マップ322は不要であり、ファイルと共に記憶されることはない。ターゲティング識別のためにパブリック・プレーヤー212識別子またはプライベート・プレーヤー226識別子をヘッダに記憶することができる。プレーヤー212／226は、ライプラリ・サーバ260からデータを受信した後、プレーヤー212／226識別子またはグループ識別子がヘッダに含まれているかどうかを検査する。この方法では、未修正移動再生装置212が仮定され、コンテンツの許可されない再生を防止する場合と同じ結果が達成される。

【0039】

他の代替実施形態では、ユーザがライブラリ・サーバ260に登録しユーザのクライアントIDを得るときに、ターゲティングされた移動再生装置212のプレーヤーIDがクライアント・コンピュータ・システム214によってライブラリ・サーバ260に送信される。この代替実施形態では、このプレーヤーIDはユーザ・プロファイル内のライブラリ・サーバ260上に記憶される。この実施形態では、ライブラリ・サーバ260は、ターゲティングされた移動再生装置212のプレーヤーIDを管理する。

【0040】

デジタル署名プロトコル

本発明で使用される第3の認証プロトコルはデジタル署名プロトコルである。ライブラリ・サーバ260によって生成されクライアント・コンピュータ・システム214にダウンロードされる選択されたデータ・ブロックに対して、ライブラリ・サーバ260はそのプライベート・ライブラリ鍵263を使用してこのデータ・ブロックにデジタル署名を適用する。デジタル署名は既知のビット文字列またはデータ・パターンを含み、このビット文字列またはデータ・パターンは、ライブラリ・サーバ260からクライアント・コンピュータ・システム214にダウンロードされるデータ・ブロック内のデータと組み合わされる。ライブラリ・サーバ260は、すべてのデータ・ブロックまたはデータ・ブロックの選択されたサブセット上でこの動作を実行することができる。データ・ブロックがクライアント・コンピュータ・システム214を介してプレーヤー212/226にダウンロードされた後、プレーヤー212/226は、プレーヤー212/226に知られている公開サーバ鍵を使用して、ライブラリ・サーバ260によって適用されるデジタル署名を検索することができる。それによって、プレーヤー212/226は、データ・ブロックが許可されたライブラリ・サーバ260から発信されたことを検証すると共に、データ・ブロックの完全性を検証することもできる。公開サーバ鍵はクライアント・コンピュータ・システムにも知られており、クライアント・コンピュータ・システム214は同一の動作を実行し、データ・ブロックが許可されたライブラリ・サーバ260から発信されたことを検証

する。この実施形態では、ライプラリ・サーバ260はコンテンツ上で署名を実行する。当業者には、オーサリング・システム280によってデジタル情報にも署名を実行できることが認識されよう。署名は、オーサリング・システム280およびライプラリ・サーバ260によって共用される多重ステップ・プロセスで実行することもできる。

【0041】

代替実施形態では、信頼できるクライアント・コンピュータ・システム214によって、ダウンロードされたマテリアルにデジタル署名が適用される。他の代替実施形態では、デジタル署名は、ダウンロードされたマテリアルには適用されず、システム・セキュリティはターゲティングおよび／またはポイント・ツー・ポイント認証の使用に依存する。

【0042】

クライアント・コンピュータ・システムから移動再生装置への、デジタル情報コンテンツ、ソフトウェアの更新、または構成情報のダウンロード

第1のステップでは、クライアント・コンピュータ・システム214および移動装置は、前述のポイント・ツー・ポイント認証プロトコルを使用して、許可された移動再生装置212が許可されたクライアント・コンピュータ・システム214と通信していることを検証する。そうである場合、移動再生装置212は、そのメモリ・マップを移動装置インターフェース221を介してクライアント・コンピュータ・システム214に送信する。クライアント・コンピュータ・システム214に存在する利用可能なデジタル情報ファイル220およびプレーヤー構成プロファイルを決める目次が、クライアント・コンピュータ・システム214のユーザ用の移動再生装置212メモリ・マップと共に表示される。ユーザは、指定された移動再生装置212メモリの、移動再生装置212メモリ・マップによって決められる部分またはセグメントをクライアント・コンピュータ・システム214のどのファイル220で置き換えるべきかを選択する。別法として、この選択プロセスを自動的に実行するようにクライアント・ブラウザ219を構成することができる。いずれの場合も、ユーザが再生装置212の利用可能なメモリよりも大きなデジタル情報コンテンツを選択することは防止される。また、再

生装置 212 用の制御ソフトウェアおよび／または構成データをクライアント・コンピュータ 214 によって自動的に更新することができる。その後、指定されたデジタル情報ファイル 220、関連するヘッダ、命令コード、または構成データは、移動再生装置 212 メモリにダウンロードされる。移動再生装置 212 は、チェックサムを使用してこのダウンロードの完全性を検証する。移動再生装置 212 は、サーバ公開鍵 215、ヘッダ、およびデジタル署名を使用して、前述のようにダウンロードを認証する。ヘッダ・スクランブル解除マップは、ダウンロードされたデータをスクランブル解除するために、ターゲティングされた移動再生装置 212 によって使用される。他の実施形態では、移動再生装置 212 は、署名を認証する前に、ダウンロードされたデータをスクランブル解除し、かつ／または圧縮解除しておくことができる。デジタル情報コンテンツの各セグメントは、前述の技法を使用して独立に認証し、かつ妥当性を検査することができる。移動再生装置 212 上のデジタル情報プロンプトは、ダウンロードされたデータのヘッダに存在する目次によって指定される、ダウンロードされたデジタル情報コンテンツの所望の部分にユーザを導く。ユーザは、プレビュー・オプションを選択することによってデジタル情報コンテンツの選択された部分を確認することができる。プレビュー・オプションは、選択されたデジタル情報プログラムの所定の部分を再生する。特定のデジタル情報プログラムが選択された後、移動再生装置 212 がデジタル情報コンテンツを、オーディオ出力手段を通して再生される音声、または表示装置上に表示される表示可能な画像に変換した後で、選択されたデジタル情報プログラムがユーザに対して再生される。

【0043】

クライアント・コンピュータ・システム 214 のソフトウェア・プレーヤー 226 は、移動再生装置 212 にダウンロードされたデジタル情報コンテンツとほぼ同じ形式でデジタル情報コンテンツを受信することもできる。しかし、ソフトウェア・プレーヤー 226 用のデジタル情報コンテンツをソフトウェア・プレーヤー 226 にダウンロードする必要はない。ソフトウェア・プレーヤー 226 は、クライアント・コンピュータ・システム 214 とメモリおよび／またはディスク記憶空間を共用するので、デジタル情報コンテンツに直接アクセスすることが

できる。したがって、ダウンロードやメモリ・マップに関する問題は生じない。

ソフトウェア・プレーヤー 226 は、移動再生装置 212 の場合と同様に、デジタル署名検証、チェックサムの検証、ターゲティングされた情報の受信を行う。代替実施形態では、ソフトウェア・プレーヤー 226 は、デジタル情報コンテンツ、構成情報、および動的にダウンロードされたソフトウェアを受信する際に移動再生装置 212 の通信プロトコルと同様な通信プロトコルを使用する。

【0044】

図 4 は、本発明の代替実施形態を示す。図 4 に示すように、オーサリング・システム 280 は複数のライブラリ・サーバ 260 をサポートすることができる。各ライブラリ・サーバは特定の種類のデジタル情報コンテンツをサポートするよう構成することができる。上記で説明したのと同様に、クライアント・コンピュータ・システム 214 は、前述の認証プロセスを実行した後で、ネットワーク 240 にアクセスし任意のライブラリ・サーバ 260 からデジタル情報コンテンツを得る。この目的のために許可サーバ 270 が設けられる。図 4 に示す構成は、より分散型のアーキテクチャを実現し、それによって負荷をいくつかのサーバ・プラットフォームに分散する。多数のクライアント・コンピュータ・システム 214 を有するサイトは、ネットワーク 240 上の要求を低減するためにサイト自体のライブラリ・サーバ 260 を有することができる。このアーキテクチャは、クライアント・コンピュータ・システム 214 の数が増加し、ライブラリ・サーバ 260 から与えられるコンテンツが増大するときにうまくスケーリングすることができる。

【0045】

図 5 は本発明の他の実施形態を示す。ただし、単一のライブラリ・サーバ・プラットフォーム 461 上で並行して実行される複数の別々のプロセスまたはタスク 460 としてライブラリ・サーバ 461 が実現されている。各ライブラリ・サーバ・プロセス 460 は、デジタル情報コンテンツの対応する部分へのアクセスを求める要求を処理する。このコンテンツは、前述のようにオーサリング・システム 280 を使用して作成される。許可サーバ 270 は、クライアント・コンピュータ・システム 214 とライブラリ・サーバ・プロセス 460 との間のリンク

の妥当性を検査するために使用される。図5に示す構成は、単一のサーバの都合が維持され、同時に複数のライブラリのスケーラビリティもサポートされるという点で有利である。

【0046】

この概念は、オーサリング・サーバ280および許可サーバ270のそれぞれに使用することもできる。図6に示すように、オーサリング・システム280および許可サーバ270は、単一のプラットフォーム685上でオーサリング・プロセス680および許可プロセス670として実現される。これらのプロセスは、上記と同じ機能を実行する。ただし、この実装では、単一のサーバの都合が図られ、オーサリング・タスクおよび許可タスクに関する複数のプロセスのスケーラビリティが実現される。

【0047】

図7は、クライアント・コンピュータ・システム214がローカル・ライブラリ710を含む他の代替実施形態を示す。ローカル・ライブラリ710は、ローカル記憶領域ライブラリ・アクセス制御機能を実現し、この機能は、ライブラリ・サーバ260から保存デジタル情報のサブセットへのアクセスを可能にする。前述のように、クライアント・コンピュータ・システム214のユーザは、ユーザがアクセスする必要のあるライブラリ・サーバ260内のデジタル情報のタイトルまたはアイテムを識別する。好ましい実施形態では、選択されたこのコンテンツは、(図2に示すように)クライアント記憶領域220に転送され、それに続いて移動再生装置212にダウンロードされる。図7に示す実施形態は、クライアント記憶領域220を拡張し、ローカル・ライブラリ710を作成する。ローカル・ライブラリ710は、選択されたコンテンツを記憶するために使用され、ローカルに記憶されたコンテンツを探索し、ソートし、分類し、抽象化するためにも使用される。ローカル・ライブラリ710は、クライアント・コンピュータ・システム214が完全なライブラリの小さなサブセットを維持することを可能にし、ユーザが選択した様々な構成のコンテンツのカスタム集合を作成するためにこのサブセットを使用することができる。クライアント・システム214は、他のクライアント・システム214上のローカル・ライブラリ710のコンテ

ントにアクセスすることができる。関連する代替実施形態では、ライブラリ・サーバ・プロセス 460 は、選択されたクライアント・システム 214 上に存在することもできる。この実施形態によって、クライアント・システム 214 は、コンテンツをブラウズし購入することができる。このコンテンツは、スクランブルされ、ターゲティングされ、ローカルに配置されたクライアント・システム 214 上で実行されるライブラリ・サーバ・プロセス 460 から供給される。ライブラリをローカルに維持することによって、ネットワーク・アクセスおよび転送オーバヘッドの一部がなくなる。

【0048】

図 8 は、本発明の他の代替実施形態を示す。この場合、クライアント・コンピュータ・システム 214 がなくなり、移動再生装置 212 がネットワーク・インターフェース 810 を介してネットワーク 240 に直接接続される。好ましい実施形態では、移動再生装置 212 は、主として、オーディオ・ファイルの再生専用あるいは表示装置上でのビジュアル画像またはテキストの表示専用の、最小限の機能を有する装置である。移動再生装置 212 は、軽量で低コストで容易に移動できる特徴を保持するように最小限の構成を有する。したがって、好ましい実施形態は、ポータブル・パーソナル・コンピュータまたはラップトップ・コンピュータの使用を含まない。というのは、このような装置は従来、好ましい移動再生装置 212 の軽量制約および低コスト制約に従わないからである。しかし、最小限の移動再生装置 212 は、従来型のハードウェア・コネクタ、ハードウェア・バッファおよびコントローラ、ならびに特定の従来型のネットワーク・プロトコルに対するファームウェア・サポートを備えるネットワーク・インターフェース 810 を追加するよう強化することができる。たとえば、移動再生装置 212 は電話ジャックを含む一体型モジュールで拡張することができる。この電話ジャックを用いて、再生装置を電話網に接続することができる。当業者には、移動再生装置 212 など低コストで軽量の装置でネットワーク・インターフェース 810 を実現できることが明らかであろう。図 8 に示す代替実施形態では、クライアント・システム・ブラウザ 219 を使用できないので、移動再生装置 212 ファームウェアまたはその他の非揮発性メモリに簡略化されたユーザ・インターフェースを設け

ることができ、ユーザは、このユーザ・インターフェースを用いて、ライブラリ・サーバ260からダウンロードし再生すべきデジタル情報アイテムを選択することができる。前述のように、ユーザがライブラリ・サーバ260コンテンツにアクセスする前に移動再生装置212とライブラリ・サーバ260との間のリンクの妥当性を検査する認証プロセスも実行しなければならない。別法として、クライアント・ブラウザ219をサポートし、それによって、ライブラリ・サーバ260から任意の移動再生装置212に直接ダウンロードし再生すべきデジタル情報アイテムを選択できるようにするために、ネットワーク240に結合されたクライアント・システム814を設けることができる。クライアント・システム814は、デジタル情報、ソフトウェア、および構成データを、記憶空間220またはローカル・ライブラリ710と同様な形式でローカルに記憶することをサポートすることができる。また、ネットワーク240を介してライブラリ・サーバ260ではなくクライアント・システム814と通信する、ネットワーク・インターフェース810のより簡略化された実装を設計することができる。

【004.9】

本発明の他の代替実施形態では、前述のようにクライアント・コンピュータ・システム214およびライブラリ・サーバ260を使用して、デジタル情報プログラミングが選択される。しかし、選択されたプログラミングは大容量記憶媒体241上で供給される。大容量記憶媒体241は、CD-ROM、PCMCIAカード、DVD、フロッピイ・ディスク、着脱可能ハード・ドライブ、デジタル磁気テープ、光カード、フラッシュ・メモリ、あるいはその他の光メモリ装置、磁気メモリ装置、電子メモリ装置、または半導体メモリ装置を含む様々な従来型の大容量記憶技法のうちの任意の技法を表わす。ユーザがクライアント・コンピュータ・システム214を選択すると、選択されたプログラミングが、前述のようにターゲティングされスクランブルされ、選択された大容量記憶媒体241に転送され、郵送されるか、あるいは手渡しされるか、あるいはユーザによって取り出せるように保持される。ユーザが、選択された大容量記憶媒体241を物理的に所有した後、選択されたプログラミングは、前述のように、クライアント・ブラウザ219によって大容量記憶媒体241から読み取り、その後移動再生裝

置212に転送することができる。図9は、クライアント・コンピュータ214を使用した移動再生装置212へのデータ転送を含まないシステムの他の実施形態を示す。キオスク910は前述の図1で示されるようなコンピュータ・システムから構成される。キオスク910は、公的にアクセスできるユニットであり、クライアント・コンピュータ・システム214と同様にブラウズ機能、コンテンツ購入機能、およびダウンロード機能を実行することができる。キオスク910は、コンテンツの高速ローカル・アクセスおよびダウンロードができるようにそれ自体のライプラリ・サーバを含むので特殊なシステムである。キオスク910は、移動装置インターフェース221、すなわち、クライアント・ブラウザ219の特殊バージョンと、ローカル・ライプラリ・サーバ・プロセス460とを含む。キオスク・ライプラリ・サーバ・プロセス460は、スクランブルされ圧縮されたデジタル情報ファイル262をローカルに記憶する。このような圧縮された情報ファイル262は、リモート・オーサリング・システム280から発信され、大容量記憶媒体241の物理的トランスポートまたは配信網240を介して供給することができる。顧客は、クライアント・ブラウザ219を操作してデジタル情報ファイルをブラウズし、選択し、購入し、このデジタル情報ファイルが顧客の移動再生装置212に供給される。ネットワーク240を介してリモート許可サーバ270に接続されたライプラリ・サーバ・プロセス460によって、認証プロセス、ターゲティング・プロセス、およびダウンロード・プロセスがキオスク内で実行される。関連実施形態で、図7は、ローカル・ライプラリ710を含むクライアント・システム214を示し、このクライアント・システム214は、キオスク910と同様な機能を有するキオスクに変換することができる。このシステムでは、クライアント・ブラウザ219の特殊バージョンが前述のキオスク実施形態と同じ機能を実現する。

【0050】

システムの代替実施形態は、共通の通信網を使用してすべてのシステム構成要素を接続する。図10で、ネットワーク240はクライアント・システム214および814、ネットワーク・インターフェース810、ライプラリ・サーバ260、許可サーバ270、およびオーサリング・システム280に直接結合される

。当業者には、システムの機能を変更せずに、ネットワーク240をいくつかの独立のネットワークまたは通信リンクにセグメント化することもできることが認識されよう。

【0051】

前述のように、移動再生装置212は、許可されたデジタル情報コンテンツのみを再生することが期待される。各移動再生装置212に固有のプレーヤーIDが埋め込まれる。各移動再生装置212は任意選択で1つまたは複数のグループID値を備えることができる。候補デジタル情報ファイルには1つまたは複数のプレーヤーIDおよびグループIDが組み込まれる。移動再生装置212の組込みソフトウェアは、候補デジタル情報ファイルに埋め込まれたプレーヤーIDおよびグループIDのリストを検査し、少なくとも1つのプレーヤーIDまたはグループIDが移動再生装置212プレーヤーIDまたはグループIDと一致する場合、移動再生装置212はデジタル情報ファイルを再生する。一致が見つからない場合、移動再生装置212はデジタル情報ファイルを再生しない。

【0052】

移動再生装置212へのプレーヤーIDの割当ては好ましくは、移動再生装置212の製造時に行われる。移動再生装置212へのグループIDの割当ては、様々な理由で様々な時間に行うことができる。通常、デジタル情報ライブラリからデジタル情報ファイルにアクセスするユーザには、ユーザのアカウントに関連する単一のグループIDが割り当てられ、このグループIDはユーザの移動再生装置に埋め込まれる。グループIDは、ある会社によって維持されている装置に対応する再生装置群、あるいは単一のアカウント保持者の再生装置群、あるいは特殊利益団体またはクラブの会員によって所有されているプレーヤーに埋め込むことができる。

【0053】

実際には、ユーザがあるデジタル情報ファイルへのアクセスを購入したときと、このデジタル情報ファイルの特殊バージョンをユーザが利用できるようになったときに、ユーザのアカウント特有のグループIDがこのデジタル情報ファイルに埋め込まれる。

【0054】

埋め込まれたプレーヤーIDおよびグループIDを有する特定のデジタル情報ファイルをターゲティングの趣旨を覆すように変更できないように、図11に示すように、デジタル署名標準(DSS)を使用するセキュリティ方式を実現することが好ましい。1101で、ターゲティングすべきデジタル情報ファイルのヘッダに適切なプレーヤーIDおよびグループIDが組み込まれる。1103で、プログラム・データのn秒ごとに、安全ハッシュ・アルゴリズム(SHA)を使用する安全ハッシュが算出される。1105で、ターゲティング中のデジタル情報ファイルに関連する関連データを含むデジタル署名メッセージが作成される。このような情報には以下の情報アイテムを含めることができるが、これらに限らない。

- プログラム・ヘッダ・バージョン番号
- ハッシュ・アルゴリズム・バージョン番号
- プログラム通し番号
- ハッシュ・ロック・サイズ
- プレーヤーIDカウント
- グループIDカウント
- グループIDリスト
- ハッシュ・テーブル・カウント
- ハッシュ値

【0055】

本発明との適合性を失わずに、上記のリストにエントリを追加するか、あるいは上記のリストからエントリを削除できることが認識されよう。1107で、デジタル署名認証(DSA)に関するメッセージが与えられ、1109で、結果として得られるデジタル署名がデジタル情報ファイルに埋め込まれる。

【0056】

DSAを使用する好ましいプレーヤー・セキュリティ方式を図12に示す。1201で、プログラム・ファイル・ヘッダ、ヘッダ署名、メッセージ、およびプログラム・データの一部がプレーヤーに転送される。プレーヤーは、情報を受信

した後、1203でDSAを実行し、送信側、通常はライブラリ・サーバによつて作成された署名を認証する。首尾よく認証された場合、プレーヤーは1205で、プレーヤーのプレーヤーIDおよびグループIDを、メッセージに埋め込まれたリストと比較する。少なくとも1つのプレーヤーIDまたはグループIDが一致する場合、プレーヤーは1207で、ライブラリ・サーバからプレーヤーに転送されるプログラム・データのn秒部分ごとに安全ハッシュを算出する。算出される各ハッシュがメッセージに存在する場合、プレーヤーは1209で、プログラム・データを再生する。本発明との適合性を失わずにDSA以外の他のプレーヤー・セキュリティ方式を使用できることが認識されよう。たとえば、プログラム・データが確実に、許可された供給源から発信された有効なデータになるように、プライベートを暗号化アルゴリズムと共に使用することができる。

【0057】

したがって、認証プロトコルおよび暗号化プロトコルを使用したコンピュータ・ネットワーク・ベースのデジタル情報ライブラリ・システムを実現し、デジタル情報ライブラリ・プログラム、ソフトウェア、および構成データをクライアント・コンピュータ・システムおよびクライアント・コンピュータ・システムに着脱可能に接続できる移動デジタル情報再生装置に安全に転送する方法および装置を開示した。特定の例およびサブシステムに関して本発明を説明したが、当業者には、本発明がこれらの特定の例またはサブシステムに限らず、他の実施形態にも拡張されることが明らかになろう。本発明は、特許請求の範囲に指定されるすべてのこれらの他の実施形態を含む。

【図面の簡単な説明】

【図1】

本発明に適合する典型的なコンピュータ・プラットフォームを示す図である。

【図2】

本発明に適合するコンピュータ・ネットワーク・ベースのデジタル情報ライブラリ・システムのハイレベル・ブロック図である。

【図3】

本発明に適合するオーサリング・システムのハイレベル・ブロック図である。

【図4】

複数のライブラリ・サーバを有する代替実施形態を示す図である。

【図5】

複数のライブラリ・サーバ・プロセスを有する代替実施形態を示す図である。

【図6】

単一のオーサリング／許可サーバを有する代替実施形態を示す図である。

【図7】

クライアント・コンピュータ・システムがローカル・ライブラリを有する代替実施形態を示す図である。

【図8】

移動再生装置がクライアント・コンピュータ・システムの代わりに直接ネットワーク・インターフェースを有する代替実施形態を示す図である。

【図9】

選択されたプログラミングを保持し配信するためにキオスクが使用される代替実施形態を示す図である。

【図10】

すべてのシステム構成要素が共通のネットワークを介して接続される代替実施形態を示す図である。

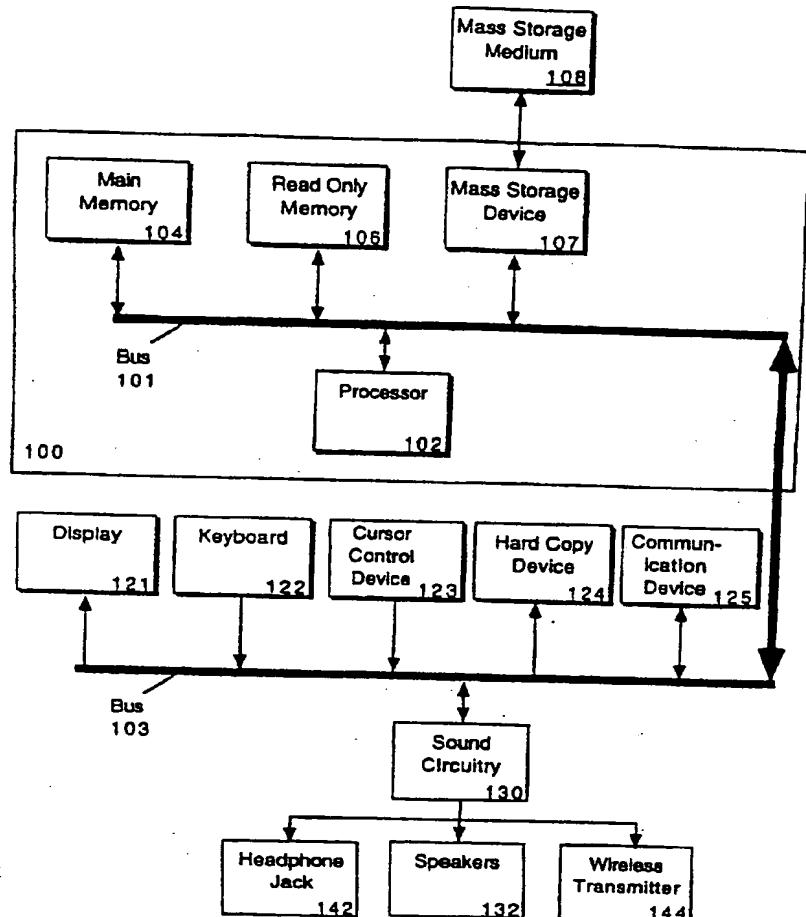
【図11】

本発明に適合するデジタル署名標準（DSS）を使用するセキュリティ方式のフローチャートである。

【図12】

本発明に適合するデジタル署名認証（DSA）を使用するプレーヤー・セキュリティ方式のフローチャートである。

【図1】



101 バス、

104 メイン・メモリ、

108 大容量記憶媒体、

123 カーソル制御装置、

130 音声回路、

142 ヘッドフォン・ジャック、

102 プロセッサ、

106 読取り専用メモリ、

121 ディスプレイ、

124 ハード・コピー装置、

132 スピーカ、

103 バス、

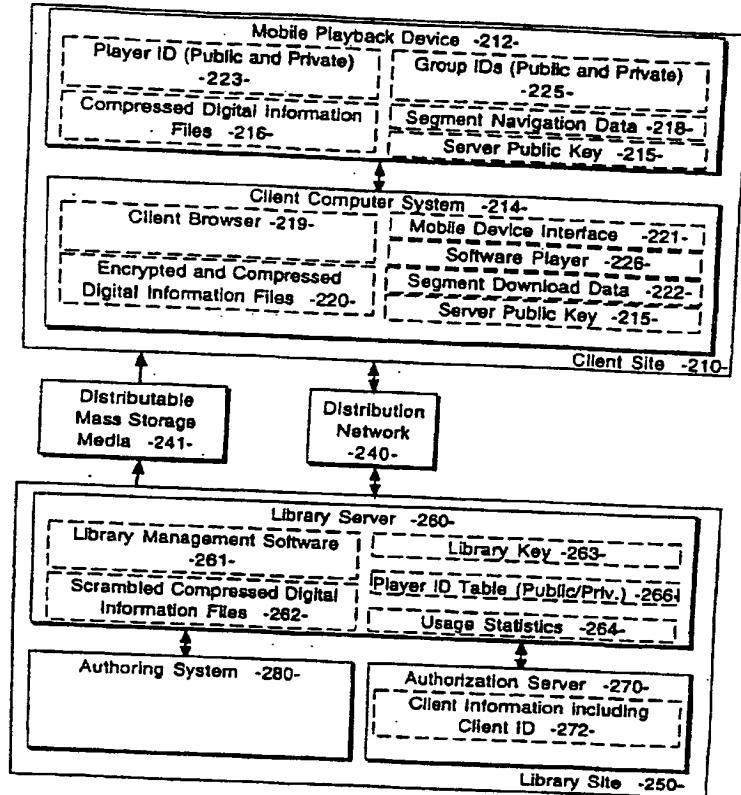
107 大容量記憶装置、

122 キーボード、

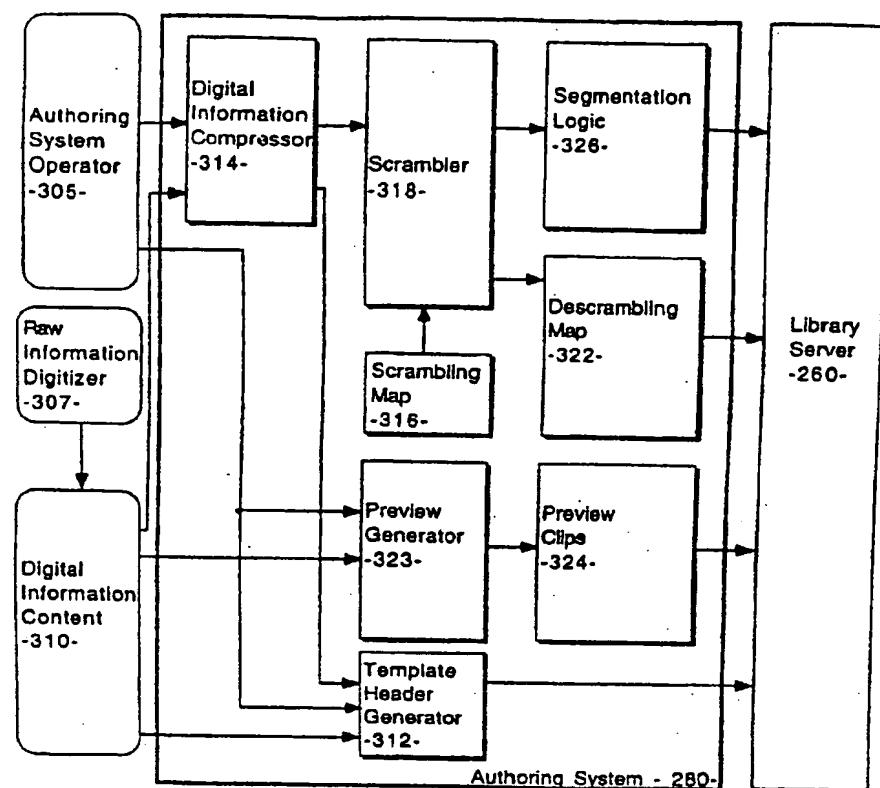
125 通信装置

144 無線送信機

【図2】

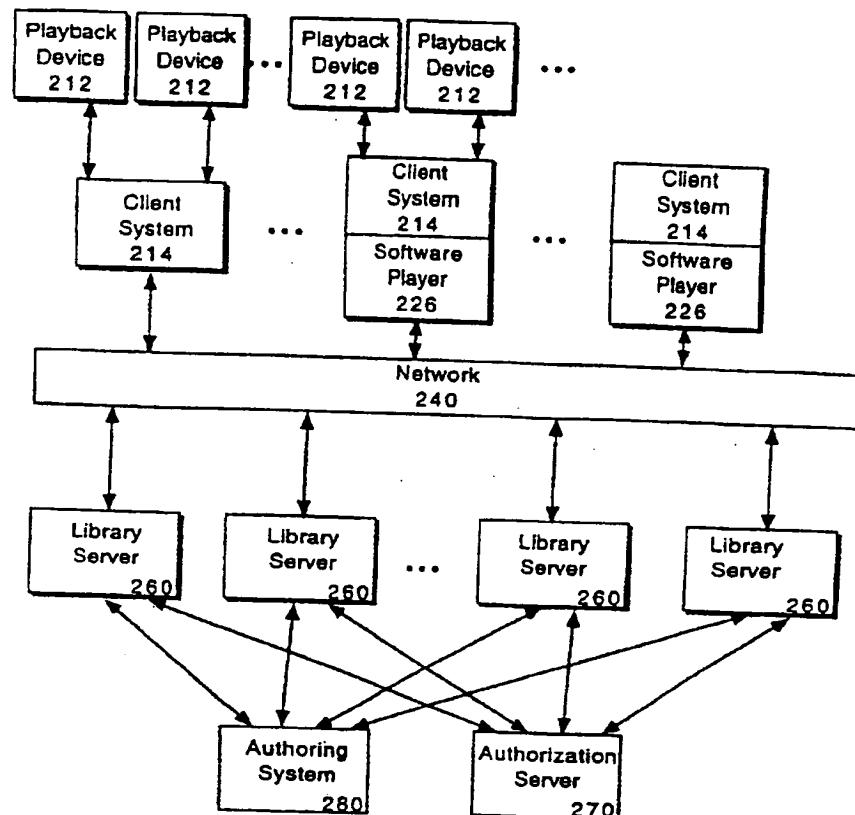


【図3】



- | | | | |
|-----|-------------------|-----|--------------|
| 260 | ライブラリ・サーバ、 | 280 | オーサリング・システム |
| 305 | オーサリング・システム・オペレータ | | |
| 307 | 生情報デジタイザ、 | 310 | デジタル情報コンテンツ |
| 312 | テンプレート・ヘッダ生成装置 | | |
| 314 | デジタル情報コンプレッサ | | |
| 316 | スクランブル・マップ、 | 318 | スクランブル |
| 322 | スクランブル解除マップ、 | 323 | プレビュー・ジェネレータ |
| 324 | プレビュー・クリップ、 | 326 | セグメント化論理 |

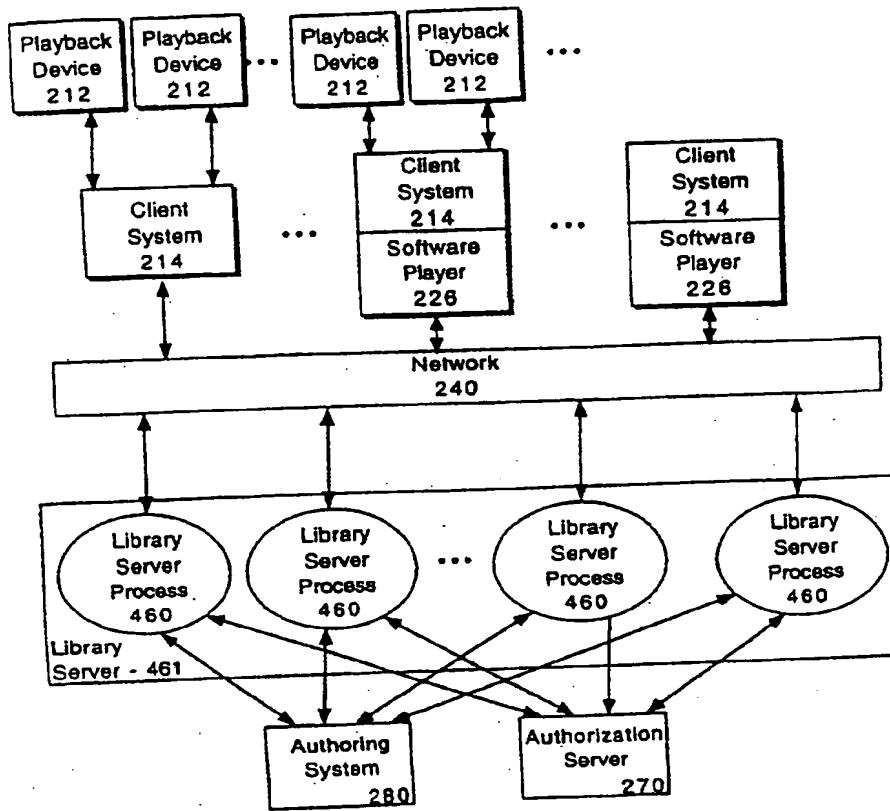
【図4】



212 再生装置、
 226 ソフトウェア・プレーヤー、
 260 ライブライ・サーバ、
 280 オーサリング・システム

214 クライアント・システム
 240 ネットワーク
 270 許可サーバ

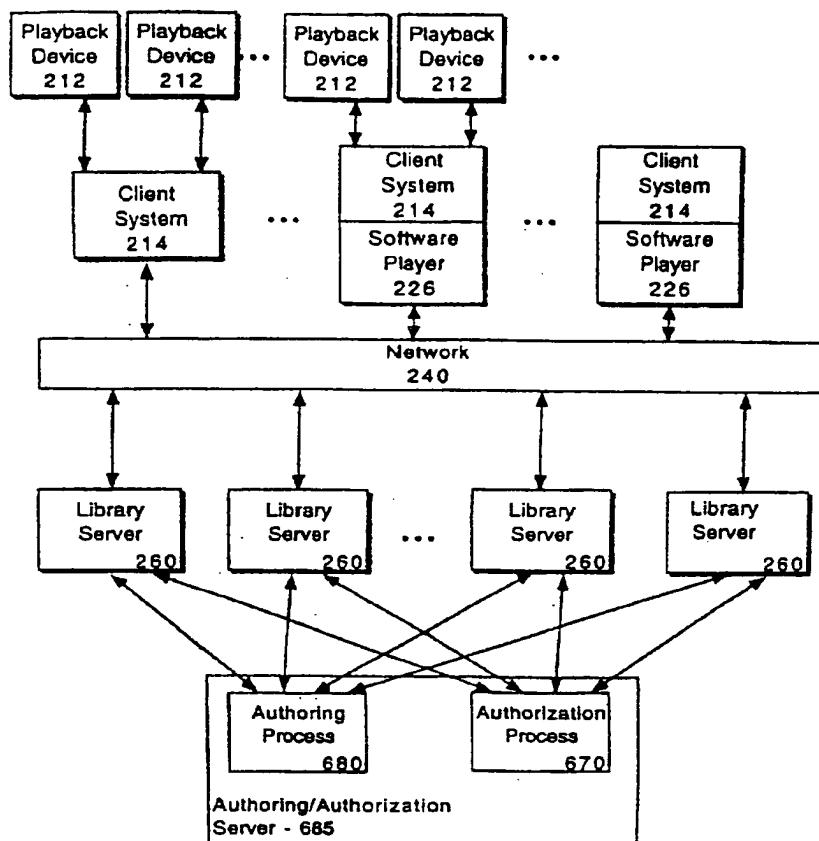
【図5】



212 再生装置、
 226 ソフトウェア・プレーヤー、
 270 許可サーバ、
 460 ライブライリ・サーバ・プロセス
 461 ライブライリ・サーバ

214 クライアント・システム
 240 ネットワーク
 280 オーサリング・システム

【図6】



212 再生装置、

226 ソフトウェア・プレーヤー、

260 ライブラリ・サーバ、

680 オーサリング・プロセス、

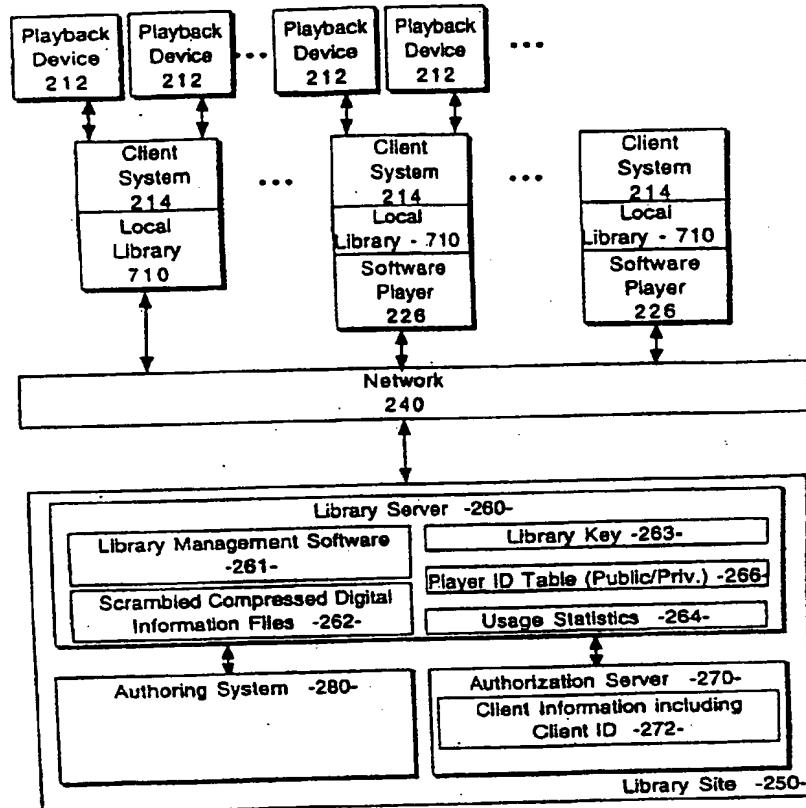
214 クライアント・システム

240 ネットワーク

670 許可プロセス

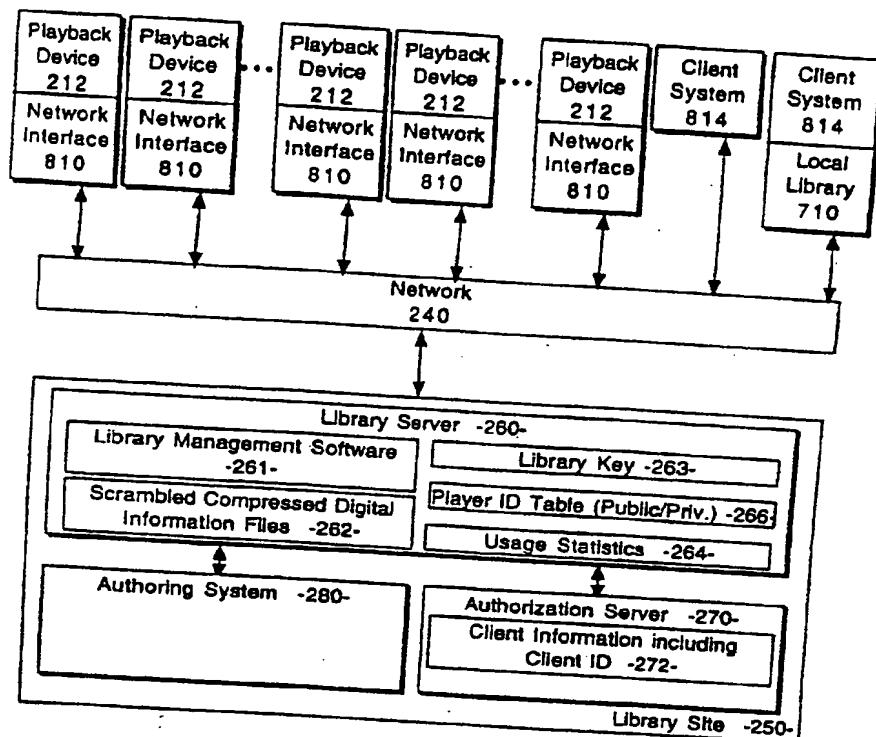
685 オーサリング／許可サーバ

【図7】



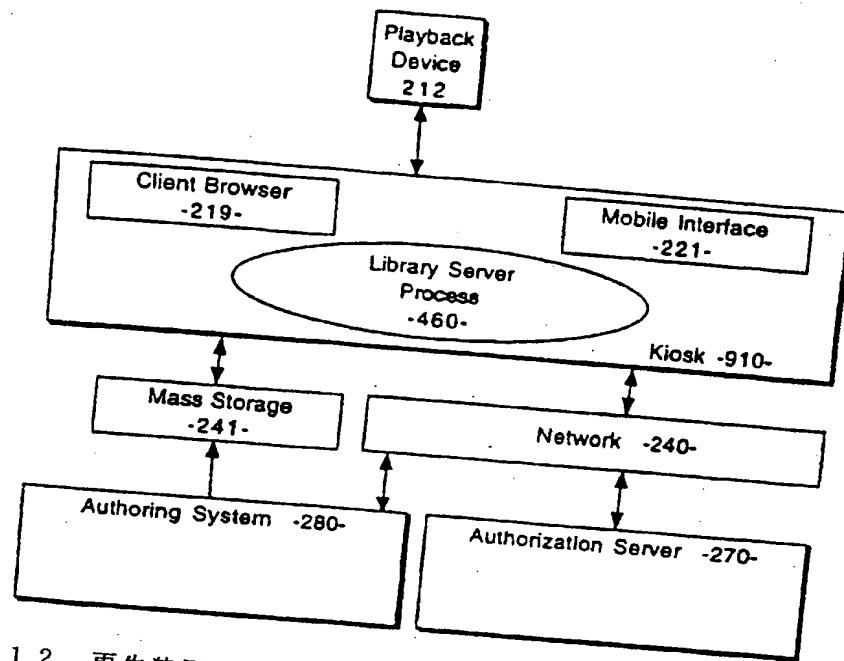
212	再生装置、	214	クライアント・システム
226	ソフトウェア・プレーヤー、	240	ネットワーク
250	ライブラリ・サイト、	260	ライブラリ・サーバ
261	ライブラリ管理ソフトウェア、	262	スクランブルされ圧縮されたデジ
263	ライブラリ鍵、	264	使用状況統計、タル情報ファイル
266	プレーヤーIDテーブル(パブリック/プライベート)		
270	許可サーバ、	272	クライアントIDを含むクライアント情報
280	オーサリング・システム、	710	ローカル・ライブラリ

【図8】



212 再生装置、
 260 ライブ・ラリ・サーバ、
 262 スクラシブルされ圧縮されたデジタル情報ファイル
 263 ライブ・ラリ・鏡、
 266 プレーヤー ID テーブル (パブリック/プライベート)
 270 許可サーバ、
 280 オーサリング・システム、
 810 ネットワーク・インターフェース、
 240 ネットワーク、
 261 ライブ・ラリ・管理ソフトウェア
 264 使用状況統計
 272 クライアント ID を含むクライアント情報
 710 ローカル・ライブ・ラリ
 814 クライアント・システム
 250 ライブ・ラリ・サイト

【図9】



212 再生装置、

221 移動インターフェース、

241 大容量記憶域、

280 オーサリング・システム

460 ライブラリ・サーバ・プロセス

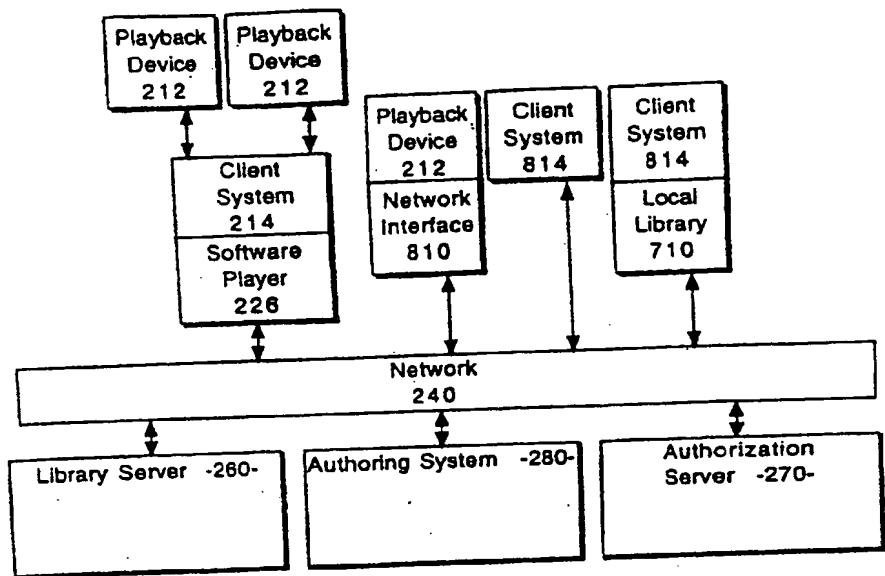
910 キオスク

219 クライアント・ブラウザ

240 ネットワーク

270 許可サーバ

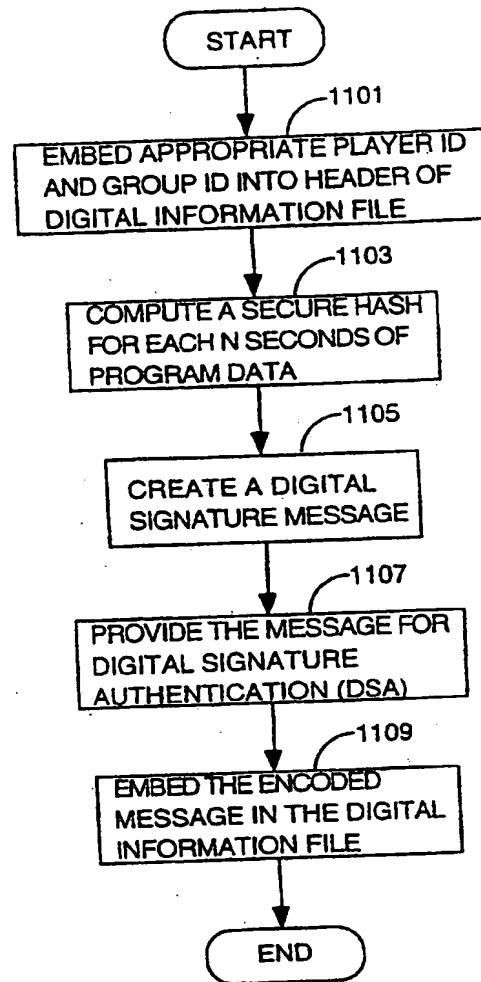
【図10】



212	再生装置、	214	クライアント・システム
226	ソフトウェア・プレーヤー、	240	ネットワーク
260	ライブラリ・サーバ、	270	許可サーバ
280	オーサリング・システム、	710	ローカル・ライブラリ
810	ネットワーク・インターフェース		
814	クライアント・システム		

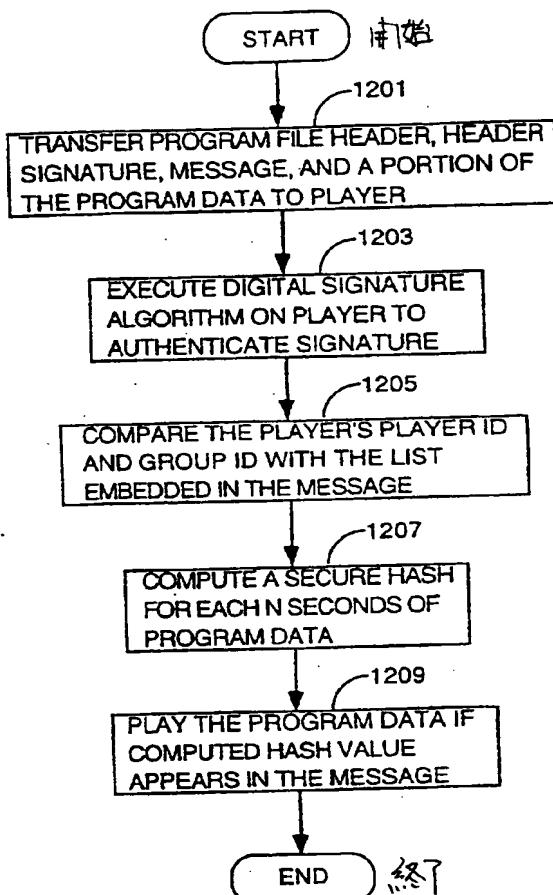
【図11】

- 1101 デジタル情報ファイルのヘッダに適切なプレーヤー ID およびグループ ID を埋め込む。
- 1103 プログラム・データの n 秒ごとに安全ハッシュを算出する。
- 1105 デジタル署名メッセージを作成する。
- 1107 デジタル署名認証 (DSA) に関するメッセージを与える。
- 1109 コード化されたメッセージをデジタル情報ファイルに埋め込む。



【図12】

- 1201 プログラム・ファイル
・ヘッダ、ヘッダ署名、
メッセージ、およびブ
ログラム・データの一
部をプレーヤーに転送
する。
- 1203 プレーヤー上でデジタ
ル署名アルゴリズムを
実行し署名を認証する。
- 1205 プレーヤーのプレーヤー
ーIDおよびグループ
IDを、メッセージに
埋め込まれたリスト比
較する。
- 1207 プログラム・データの
 n 秒ごとに安全ハッシ
ュを算出する。
- 1209 算出されたハッシュ値
がメッセージに存在す
る場合にプログラム・
データを再生する。



【手続補正書】

【提出日】平成12年5月10日(2000.5.10)

【手続補正1】

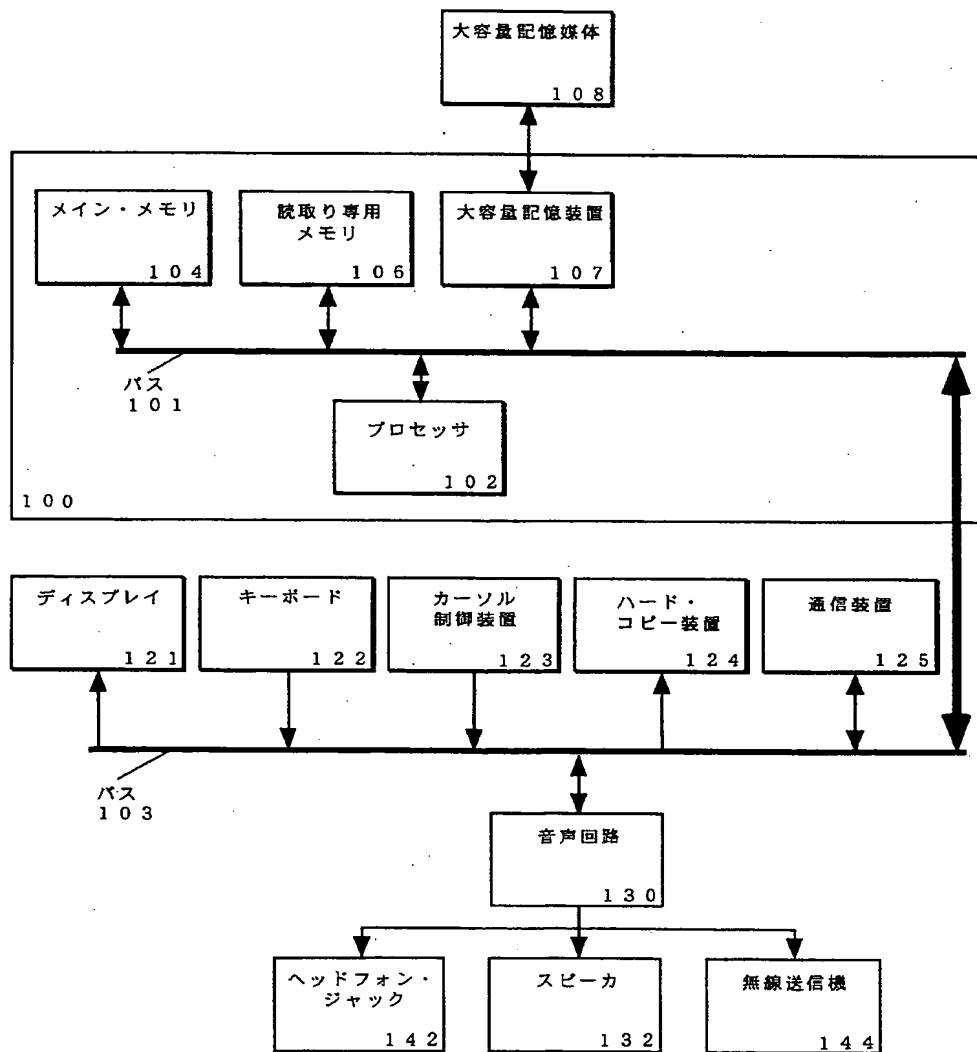
【補正対象書類名】図面

【補正対象項目名】全図

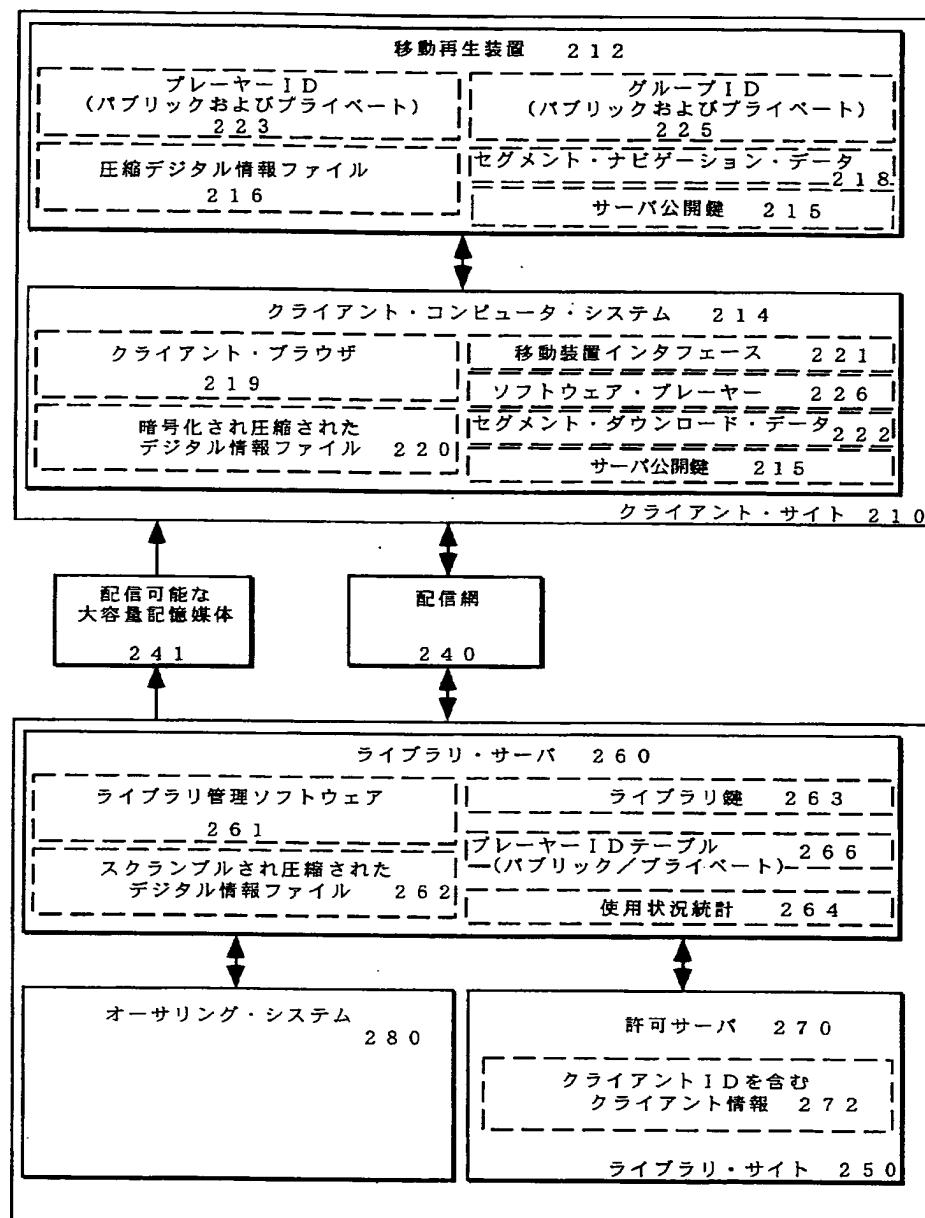
【補正方法】変更

【補正内容】

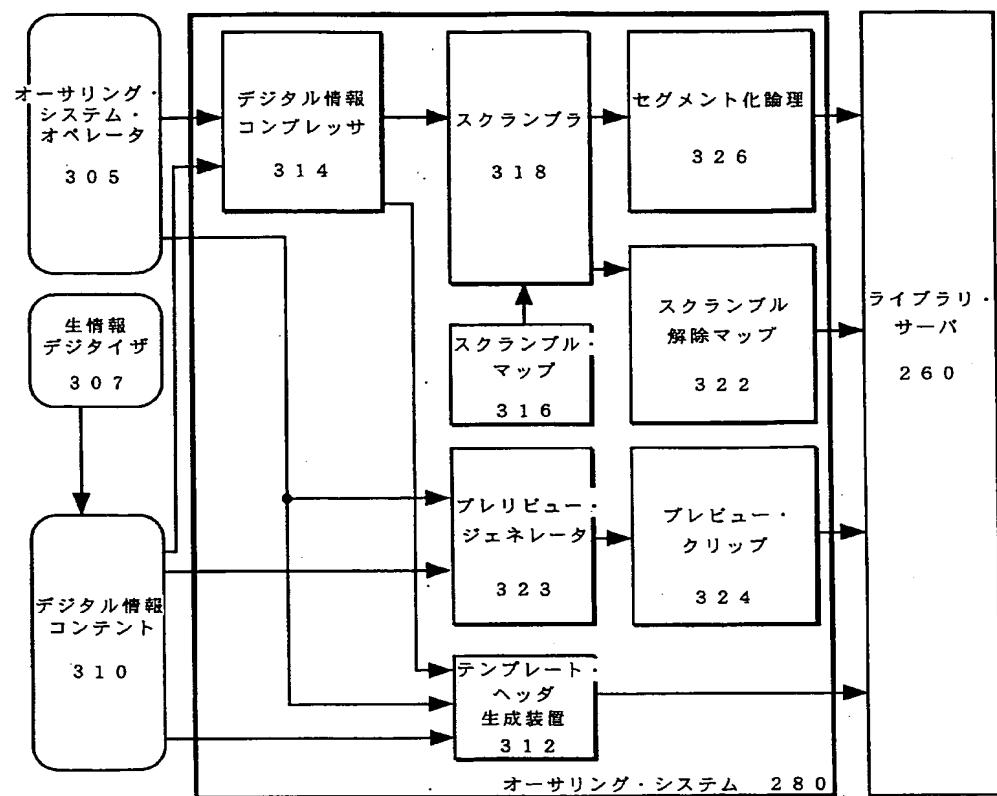
【図1】



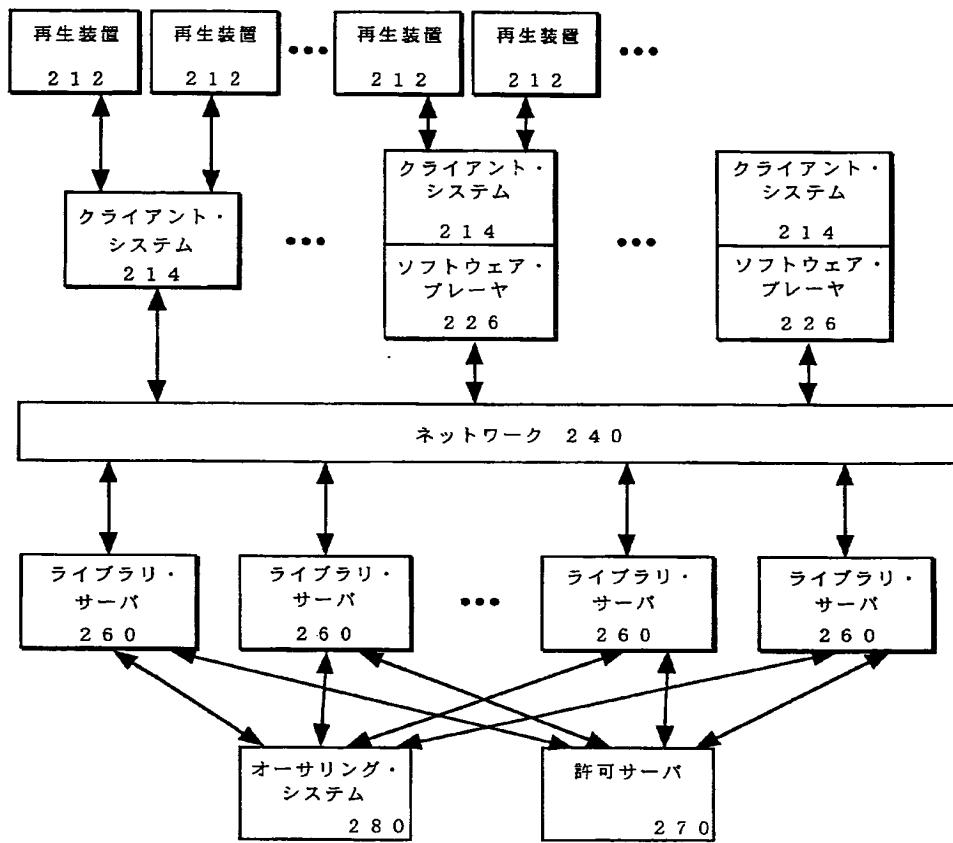
【図2】



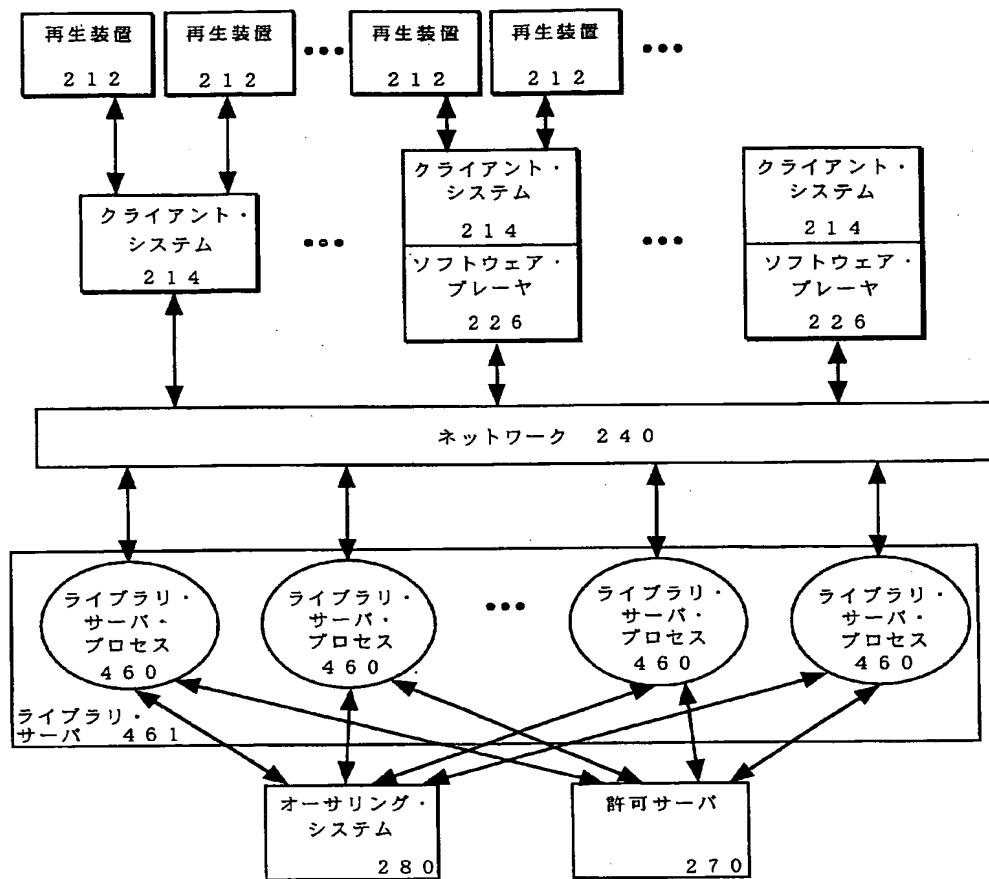
【図3】



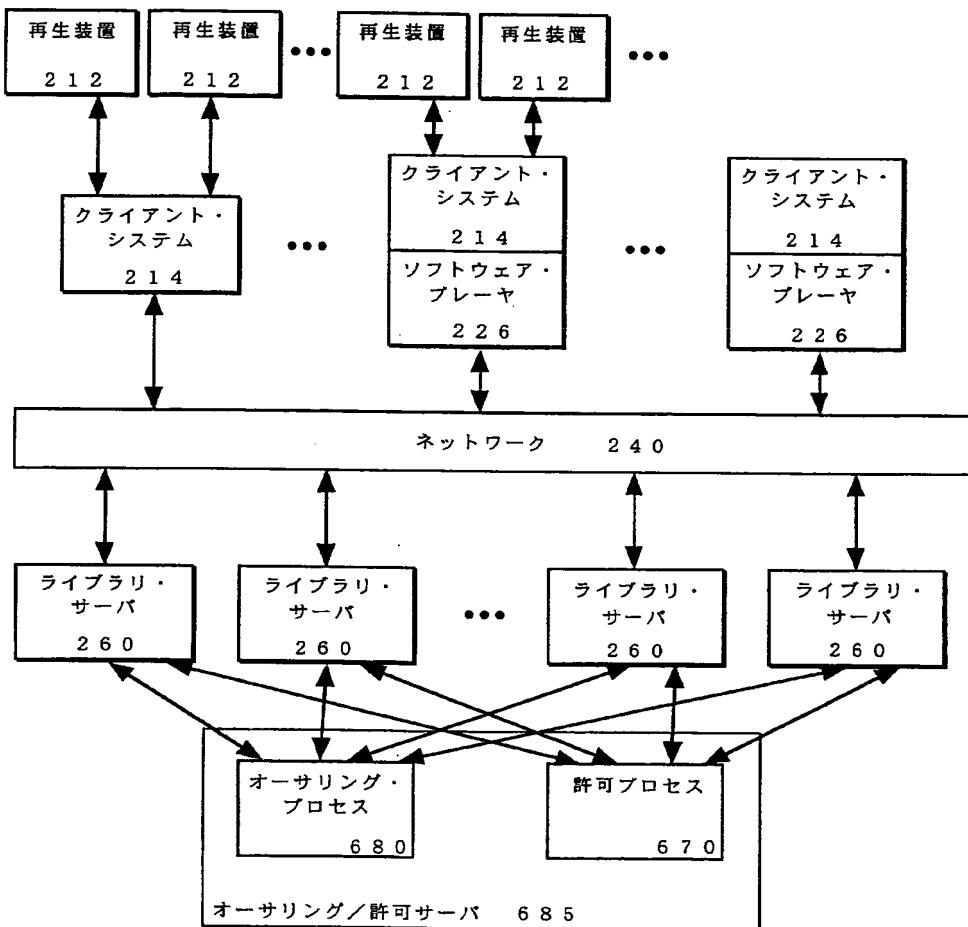
【図4】



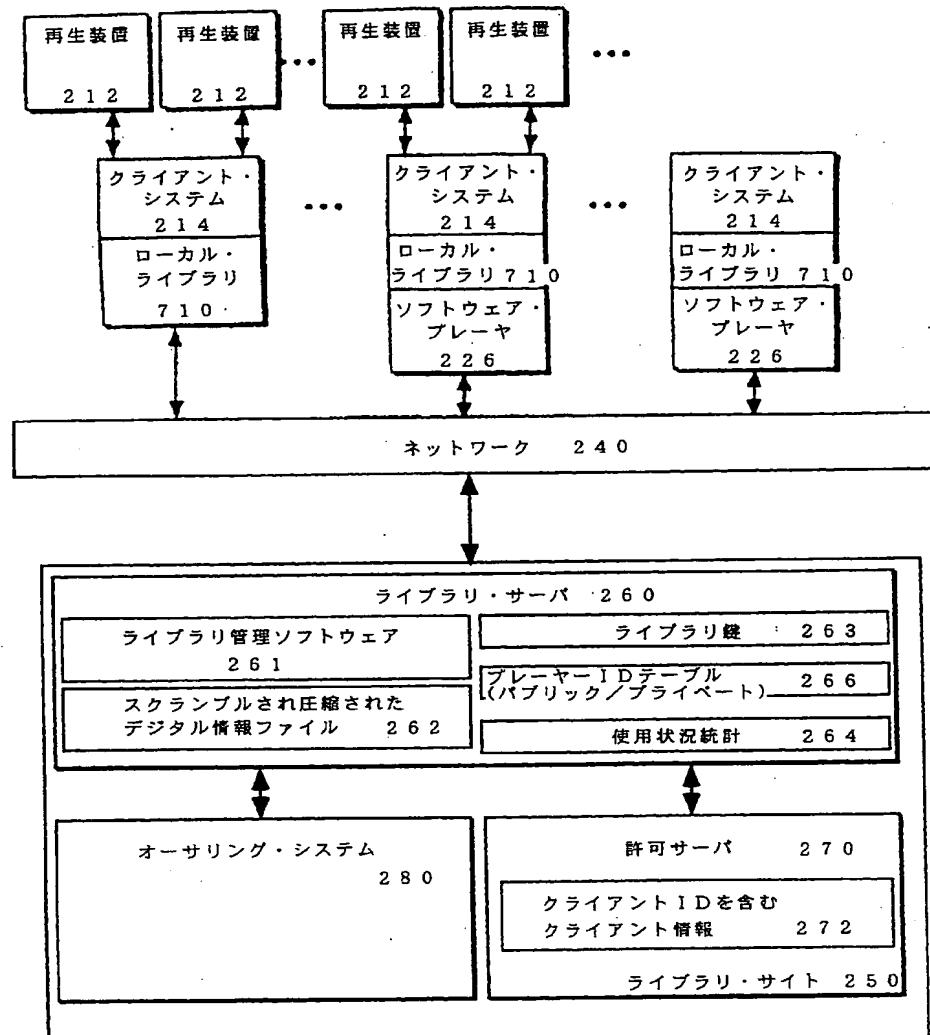
【図5】



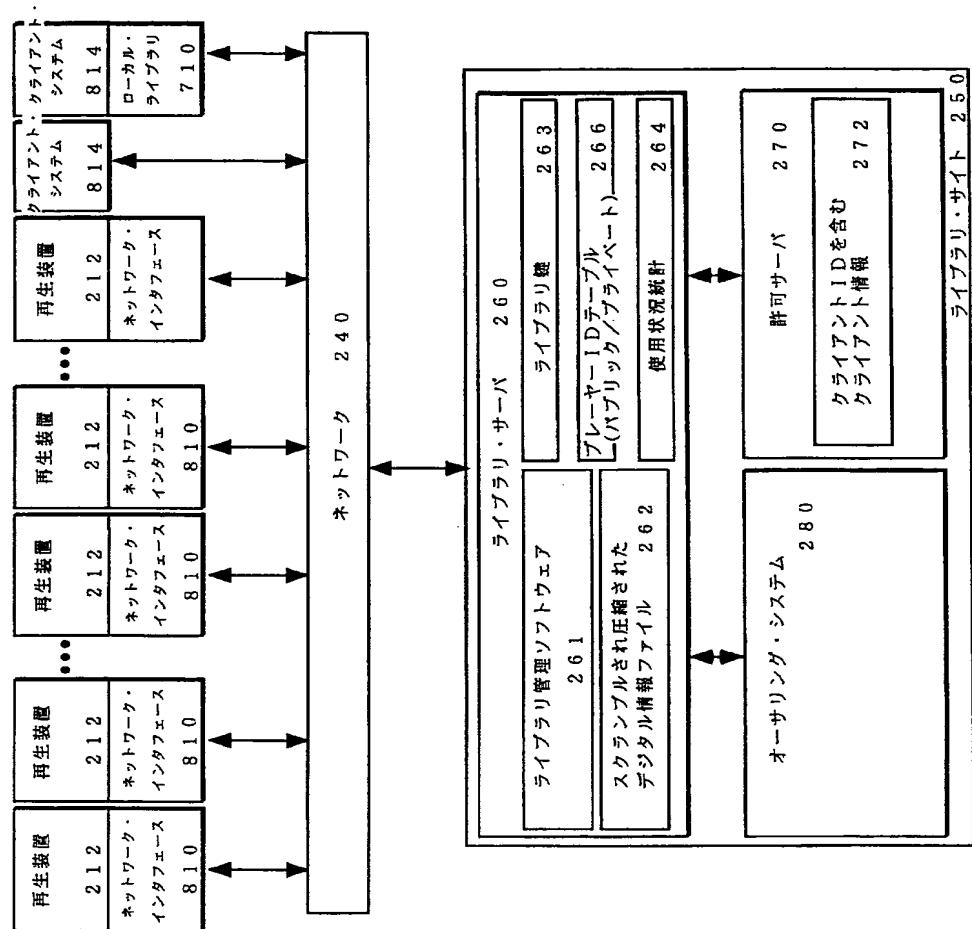
【図6】



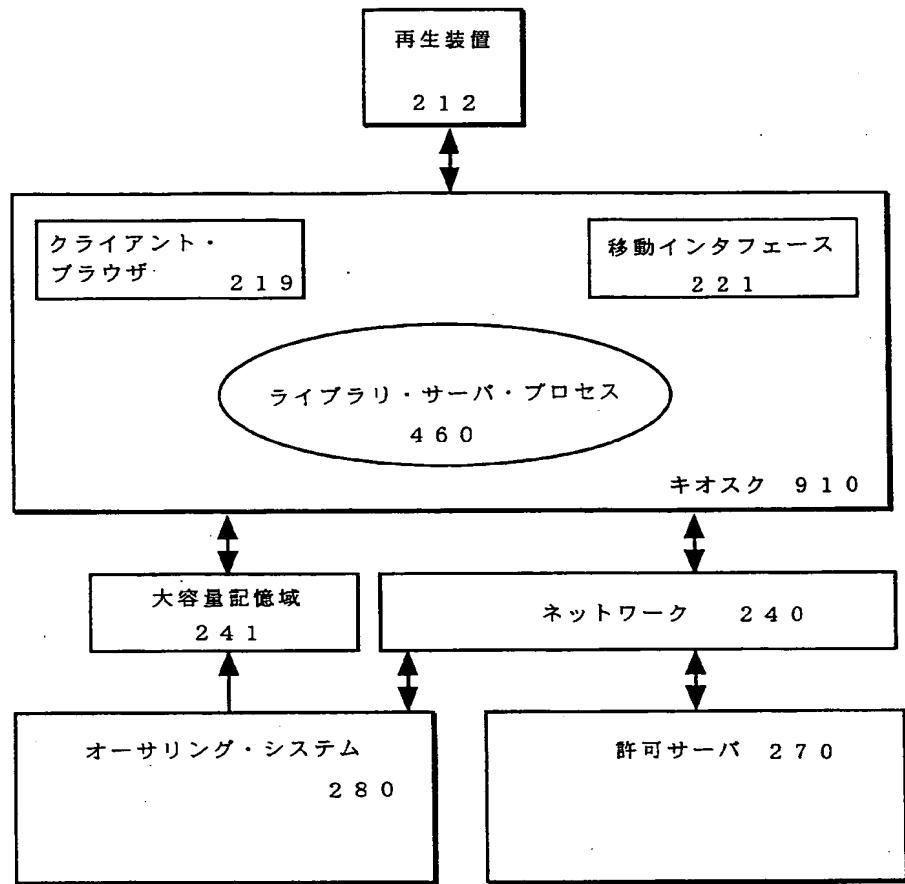
【図7】



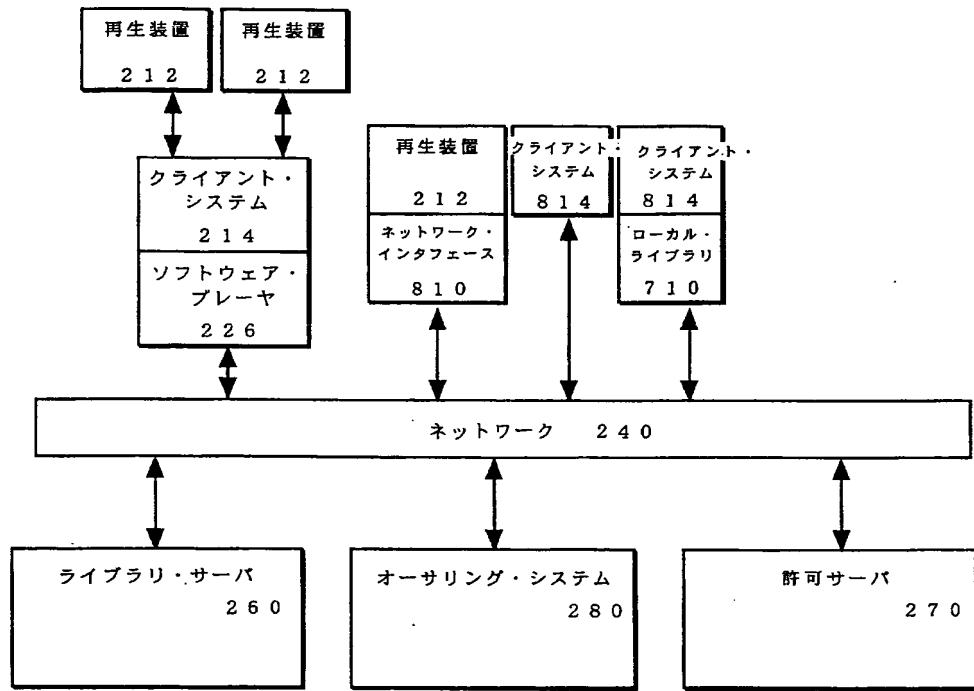
【図8】



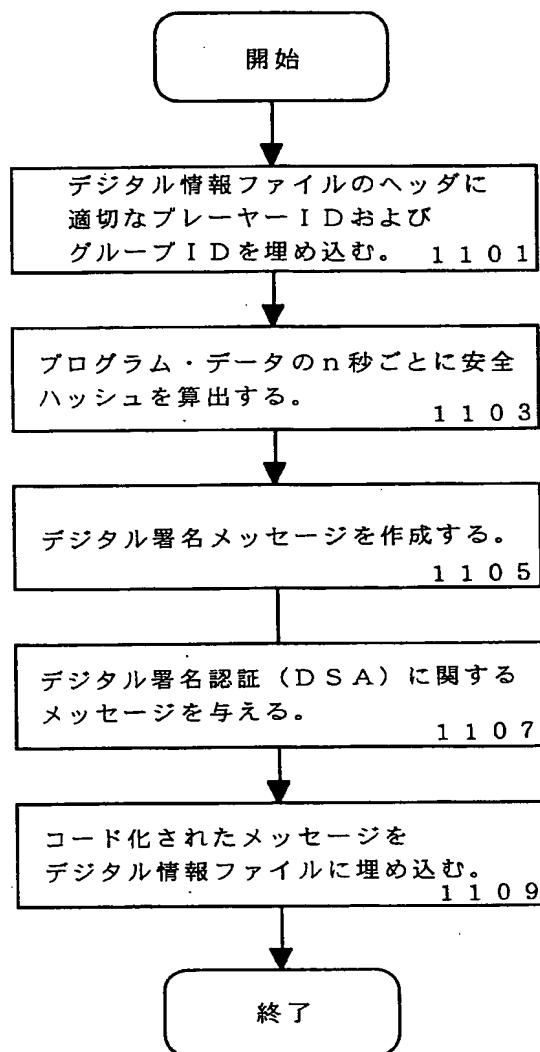
【図9】



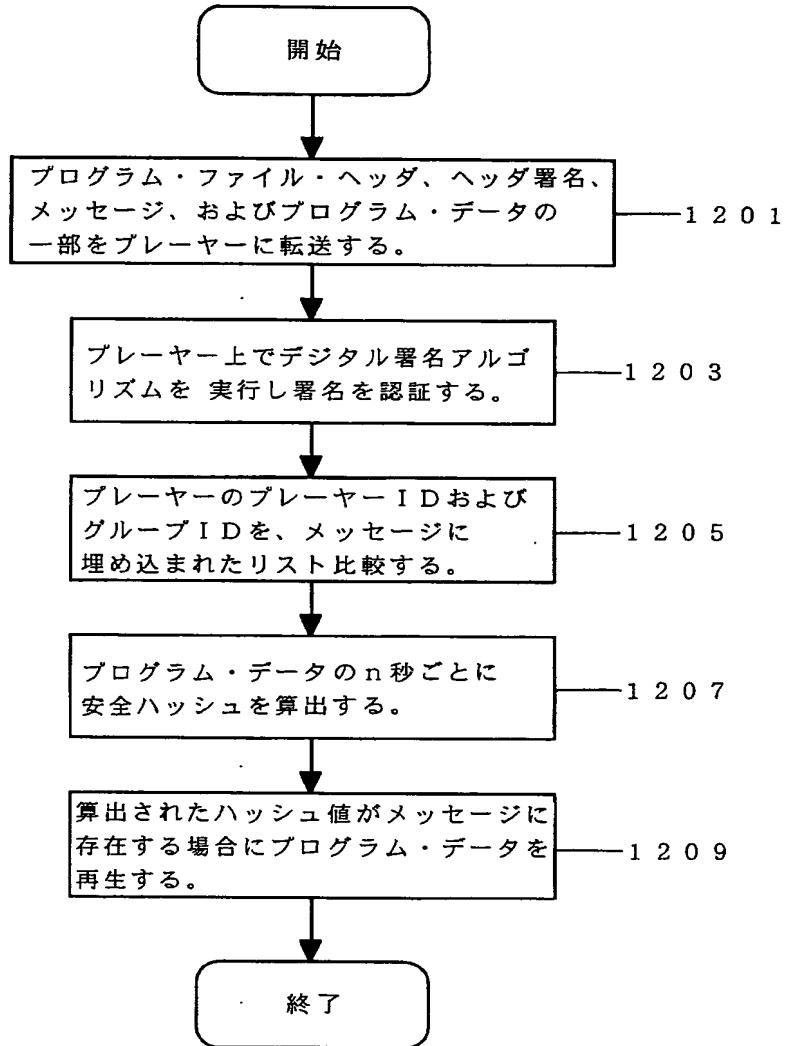
【図10】



【図11】



【図12】



【国際調査報告】

INTERNATIONAL SEARCH REPORT		international application No. PCT/US98/20659
A. CLASSIFICATION OF SUBJECT MATTER		
IPC(6) :G06F 11/00 US CL :395/186 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) U.S. : 395/186, 188.01; 380/23, 25		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Microsoft Press Computer Dictionary 2nd Edition		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) APS		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,483,658 A (GRUBE et al) 09 January 1996; Figure 1 and 2; Abstract; col. 3, lines 31-67; col. 4, lines 1-16 and 30-48; col. 5, lines 46-67; col. 6, lines 1-33.	1-2, 7-8, 13-14, 19-20, 25-26, 31-32 and 37
Y	US 5,483,658 A (GRUBE et al) 09 January 1996; Figures 1 and 2; Abstract; col. 3, lines 31-67; col. 4, lines 1-16 and 30-48; col. 5, lines 46-67; col. 6, lines 1-33.	3, 9, 15, 21, 27 and 33
Y	MICROSOFT PRESS, Computer Dictionary 2nd edition, 1994, pp. 194-195.	3, 9, 15, 21, 27 and 33
A	US 5,511,122 A (ATKINSON) 23 April 1996; see entire document.	1-37
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/>		See patent family annex.
<p>* Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document published on or after the international filing date</p> <p>"L" document which may throw doubt on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"Z" document member of the same patent family</p>		
Date of the actual completion of the international search	Date of mailing of the international search report	
29 DECEMBER 1998	24 FEB 1999	
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer ROBERT BEAUSOLIEL Telephone No. (703) 305-9713	

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT		International application No. PCT/US98/20659
C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US 5,781,723 A (YEE et al.) 14 July 1998; see entire document.	1-37
A	US 5,555,098 A (PARULSKI) 10 September 1996; see entire document.	1-37
A	US 5,132,992 A (YURT et al) 21 July 1992; see entire document.	1-37

Form PCT/ISA/210 (continuation of second sheet)(July 1992)*

フロントページの続き

(81) 指定国 EP(AT, BE, CH, CY,
 DE, DK, ES, FI, FR, GB, GR, IE, IT,
 LU, MC, NL, PT, SE), OA(BF, BJ,
 CF, CG, CI, CM, GA, GN, GW, ML,
 MR, NE, SN, TD, TG), AP(GH, GM, KE,
 LS, MW, SD, SZ, UG, ZW), EA(AM,
 AZ, BY, KG, KZ, MD, RU, TJ, TM)
 , AL, AM, AT, AZ, BA, BB, BG, BR,
 BY, CA, CH, CN, CU, CZ, DE, DK, EE,
 ES, FI, GB, GD, GE, GH, GM, HR,
 HU, ID, IL, IS, JP, KE, KG, KP,
 KR, KZ, LC, LK, LR, LS, LT, LU, LV,
 MD, MG, MK, MN, MW, MX, NO, NZ,
 PL, PT, RO, RU, SD, SE, SG, SI,
 SK, SL, TJ, TM, TR, TT, UA, UG, UZ,
 VN, YU, ZW

(72) 発明者 ジャン, ベンジャミン・チェーミン
 アメリカ合衆国・94303・カリフォルニア
 州・パロ アルト・タンランド ドライ
 ブ・1081-ビイ
 (72) 発明者 ペイ, サミュエル・ホン-イエン
 アメリカ合衆国・92009・カリフォルニア
 州・カールスバッド・ピラグア ストリー
 ト・3306
 (72) 発明者 コチャー, ポール
 アメリカ合衆国・94117・カリフォルニア
 州・サン フランシスコ・フィルモア ス
 トリート・143

F ターム(参考) 5B017 AA06 BA09 BB09 CA16
 5D044 AB01 AB05 BC01 BC02 CC04
 DE49 GK12 HL11
 5J104 AA07 AA09 AA16 EA04 EA26
 KA02 KA06 KA09 LA03 LA06
 MA02 NA12 PA11

THIS PAGE BLANK (USPTO)